Office of Technology Assessment

Congressional Board of the 99th Congress

TED STEVENS, *Alaska, Chairman*

MORRIS K. UDALL, *Arizona, Vice Chairman*

Senate

ORRIN G. HATCH
Utah

CHARLES McC. MATHIAS, JR.
Maryland

EDWARD M. KENNEDY
Massachusetts

ERNEST F. HOLLINGS
South Carolina

CLAIBORNE PELL
Rhode Island

House

GEORGE E. BROWN, JR.
California

JOHN D. DINGELL
Michigan

CLARENCE E. MILLER
Ohio

COOPER EVANS
Iowa

DON SUNDQUIST
Tennessee

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

WILLIAM J. PERRY, *Chairman*
H&Q Technology Partners

DAVID S. POTTER, *Vice Chairman*
General Motors Corp. (Ret.)

EARL BEISTLINE
Consultant

CHARLES A. BOWSHER
General Accounting Office

CLAIRE T. DEDRICK
California Land Commission

JAMES C. FLETCHER
University of Pittsburgh

S. DAVID FREEMAN
Lower Colorado River Authority

JOSEPH E. ROSS
Acting Director
Congressional Research Service

MICHEL T. HALBOUTY
Michel T. Halbouty Energy Co.

CARL N. HODGES
University of Arizona

RACHEL McCULLOCH
University of Wisconsin

LEWIS THOMAS
Memorial Sloan-Kettering
Cancer Center

Director

JOHN H. GIBBONS

The Technology Assessment Board approves the release of this report. The views expressed in this report are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

Federal Government Information Technology:

Management, Security, and Congressional Oversight

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D.C. 20510

J 952-16

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

Library of Congress Catalog Card Number 86-600507

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402

Foreword

The primary focus of this report is on the management, use, and congressional oversight of information technology in the Federal Government. Rapid advances in technology—such as microcomputers, computer networking, computer modeling, videoconferencing, and electronic information exchange—are generating many new applications, opportunities, and issues that warrant congressional attention.

The report addresses five major areas: 1) management of information technology, including strategic planning, innovation, procurement, and the information resources management (IRM) concept; 2) information systems security and computer crime; 3) information technology and decision support; 4) management of government information dissemination; and 5) opportunities for using information technology in conducting congressional oversight.

Prepared at the request of the Senate Committee on Governmental Affairs and the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, this report is the second component of the OTA assessment of "Federal Government Information Technology: Congressional Oversight and Civil Liberties." The first component, *Electronic Surveillance and Civil Liberties*, was published in October 1985. The third component, *Electronic Record Systems and Individual Privacy*, is forthcoming in 1986.

In preparing this report, OTA has drawn on working papers developed by OTA staff and contractors, the comments of participants at four OTA workshops on these topics, and the results of an OTA survey sent to over 140 agency units. Drafts of this report were reviewed by the OTA project advisory panel, officials from the U.S. Office of Management and Budget, General Services Administration, and National Bureau of Standards; the U.S. Departments of Agriculture, Commerce, Defense (including the National Security Agency), Education, Interior, State, and Transportation; the Federal Bureau of Investigation (Justice), Federal Emergency Management Agency, National Archives and Records Administration, Nuclear Regulatory Commission, and Veterans Administration; and a broad spectrum of interested individuals from other Federal agencies, the research community, and private industry.

OTA appreciates the participation of the advisory panelists, workshop participants, Federal agency officials who responded to OTA's survey and/or provided review comments, and others who helped bring this report to fruition. The report itself, however, is solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.

Federal Government Information Technology Advisory Panel

Theodore J. Lowi, *Chairman*
Professor of Political Science, Cornell University

Arthur G. Anderson
IBM Corp. (Ret.)

Jerry J. Berman
Legislative Counsel
American Civil Liberties Union

R.H. Bogumil
Past President
IEEE Society on Social Implications of Technology

James W. Carey
Dean, College of Communications
University of Illinois

Melvin Day
Vice President
Research Publications

Joseph W. Duncan
Corporate Economist
The Dun & Bradstreet Corp.

William H. Dutton
Associate Professor of Communications and Public Administration
Annenberg School of Communications
University of Southern California

David H. Flaherty
Professor of History and Law
University of Western Ontario

Carl Hammer
Sperry Corp. (Ret.)

Starr Roxanne Hiltz
Professor of Sociology
Upsala College

John C. Lautsch
Chairman, Computer Law Division
American Bar Association

Edward F. Madigan
Office of State Finance
State of Oklahoma

Marilyn Gell Mason
Director
Atlanta Public Library

Joe Skinner
Corporate Vice President
Electronic Data Systems Corp.

Terril J. Steichen
President
New Perspectives Group, Ltd.

George B. Trubow
Director, Center for Information Technology and Privacy Law
The John Marshall Law School

Susan Welch
Professor and Chairperson
Department of Political Science
University of Nebraska

Alan F. Westin
Professor of Public Law and Government
Columbia University

Langdon Winner
Associate Professor of Political Science
Rensselaer Polytechnic Institute

Congressional Agency Participants

Robert L. Chartrand
Senior Specialist
Congressional Research Service

Robert D. Harris
Deputy Assistant Director for Budget Analysis
Congressional Budget Office

Kenneth W. Hunter
Senior Associate Director for Program Information
U.S. General Accounting Office

OTA Federal Government Information Technology Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Frederick W. Weingarten, *Communication and Information Technologies Program Manager*

Project Staff

Fred B. Wood, *Project Director*
Jean E. Smith, *Assistant Project Director*
Jim Dray, *Research Analyst*
Priscilla M. Regan, *Analyst*
Jennifer Nelson, *Research Assistant*

Administrative Staff

Elizabeth A. Emanuel, *Administrative Assistant*
Shirley Gayheart,* *Secretary*
Audrey Newman, *Secretary*
Renee Lloyd, *Secretary*
Patricia Keville, *Clerical Assistant*

Contractors

Rex V. Brown, *Decision Science Consortium, Inc.*
Stephen E. Frantzich, *Congressional Data Associates*
Henry H. Hitchcock, Lisa Heinz, and J.F. Coates, *J.F. Coates, Inc.*
John Leslie King and Kenneth L. Kraemer, *Irvine Research Corp.*
John C. Kresslein, *The University of South Carolina*
Karen B. Levitan, Patricia D. Barth, and Diane G. Shook, *The KBL Group, Inc.*
Charles R. McClure and Peter Hernon, *Information Management Consultant Services, Inc.*
Robert Miewald, Keith Mueller, and Robert Sittig, *The University of Nebraska*
Sanford Sherizen, *Data Security Systems, Inc.*

---

*Deceased, Dec. 11, 1985.

OTA Information Technology Management, Planning, and Procurement Workshop

Walter Anderson
U.S. General Accounting Office

Frank Carr
U.S. General Services
Administration

Robert L. Chartrand
Congressional Research Service
Library of Congress

Whit Dodson
International Data Corp.

Forest Woody Horton, Jr.
Information Consultant

John Leslie King
Irvine Research Corp.

Kenneth L. Kraemer
Irvine Research Corp.

Donald A. Marchand
University of South Carolina

Frank McDonough
U.S. General Services
Administration

John McNicholas
U.S. Office of Management and
Budget

James Pivonka
Internal Revenue Service

Harry Pontius
U.S. Department of Defense

Thomas Pyke
National Bureau of Standards
U.S. Department of Commerce

Joe Skinner
Electronic Data Systems Corp.

Robert Woods
Federal Aviation
Administration

OTA Information Systems Security and Computer Crime Workshop

Louise Becker
Elgin Group, Ltd.

David Elliott Bell
National Computer Security
Center

Kier Boyd
Federal Bureau of Investigation

Sheila Brand
National Computer Security
Center

Joseph Coates
J.F. Coates, Inc.

Whitfield Diffie
Bell Northern Research

John Martin Ferris
U.S. Department of the
Treasury

David Geneson
U.S. Department of Justice

Richard Guilmette
Prime Computer Corp.

Stuart Katzke
National Bureau of Standards
U.S. Department of Commerce

Stan Kurzban
IBM Corp.

John Lane
U.S. Department of Defense

Steve Lipner
Digital Equipment Corp.

Robert Morris
Bell Laboratories

Donn Parker
SRI Computer Security
Program

Marvin Schaefer
National Computer Security
Center

Miles Smid
National Bureau of Standards
U.S. Department of Commerce

Richard Solomon
Massachusetts Institute of
Technology

Stephen Walker
Trusted Information Systems,
Inc.

OTA Computer Modeling and Decision Support Workshop

Rex Brown
Decision Science Consortium, Inc.

Vincent Covello
National Science Foundation

Thomas Crowley
National Science Foundation

William Dutton
University of Southern California

Stephen Frantzich
U.S. Naval Academy

James Hansen
National Aeronautics and Space Administration

Alan Hecht
National Oceanic and Atmospheric Administration

Meyer Katzper
Consultant

Austin W. Kibler
U.S. Central Intelligence Agency

Jerry D. Mahlman
Princeton University

Lee Merkhofer
Applied Decision Analysis

Michael Riches
U.S. Department of Energy

Michael Schlesinger
Oregon State University

Jagadish Shukla
University of Maryland

Martin Tolcott
Decision Science Consortium, Inc.

Charles Treat
U.S. Department of Commerce

Warren Washington
National Center for Atmospheric Research

OTA Dissemination of Government Information Work Session

Sarah Bishop
National Commission on Libraries and Information Science

Michael G. Garland
Bureau of the Census

Peter Hernon
University of Arizona

Charles R. McClure
University of Oklahoma

David Peyton
Information Industry Association

Kenyon C. Rosenberg
National Technical Information Service

John Shepard
Public Citizen

Contents

Chapter *Page*

1. Summary 3
2. Trends in Federal Government Information Technology Management 13
3. Policy Issues in Management, Planning, and Innovation 43
4. Information Systems Security 59
5. Computer Crime 85
6. Computer Modeling, Decision Support, and Government Foresight 105
7. Electronic Databases and Dissemination of Government Information 139
8. Information Technology and Congressional Oversight 161

Appendix A. Other Issues 175
Appendix B. OTA Federal Agency Data Request 177
Appendix C. List of Contractor Reports 188
Appendix D. List of Outside Reviewers 189

Chapter 1
Summary

Contents

	Page
Introduction	3
Management of Information Technology	3
Strategic Planning	4
Information Availability and Data Quality	4
Innovation	4
Procurement	5
Information Resources Management (IRM)	5
Information Systems Security and Computer Crime	6
Information Systems Security	6
Computer Crime	6
Information Technology and Decision Support	7
Management of Government Information Dissemination	9
Information Technology and Congressional Oversight	10
In Conclusion	10

Chapter 1

Summary

INTRODUCTION

Information technology—including computers, software, telecommunications, and the like—is critically important to the functioning of the U.S. Government. By any measure, the Federal Government—with its roughly 27,000 mainframe computers, over 100,000 microcomputers, and over 170,000 mainframe computer terminals[1]—has the largest inventory of computer equipment of any single organization or government in the world.

However, much of the policy framework previously established by Congress to control, oversee, and encourage the management and use of Federal information technology has been overtaken by the rapid pace at which new technology applications, issues, and opportunities are being generated.

In addition, the Federal Government is not maximizing the return on its substantial information technology investment (conservatively estimated at $60 billion over fiscal years 1982-86[2]) with respect to improving: 1) the efficiency of government in delivering services; 2) the security and privacy of information maintained in computerized systems; and 3) the quality of government management itself. Also, the congressional intent as originally embodied in laws such as the Paperwork Reduction Act, Freedom of Information Act, Privacy Act, Public Printing Act, and Omnibus Crime Control Act is not being fully carried out due in part to new technological applications and issues not envisioned at the time of enactment.

---

[1] Unless otherwise noted, statistics cited in this chapter are based on the OTA Federal Agency Data Request that was sent to the 13 cabinet departments and 20 selected independent agencies, and to which 142 agency components responded. See app. B for a list.

[2] Based on Office of Management and Budget (OMB) data. Does not include some telecommunication costs or information technology activities that are classified or embedded in other agency programs.

MANAGEMENT OF INFORMATION TECHNOLOGY

The management of Federal Government information technology has received high-level congressional and executive branch attention for at least two decades, with a new round of studies, reports, and policy initiatives every several years. Management issues involving planning, procurement, security, and the like must be revisited periodically because of the dynamic nature of the technology and changing applications.

Major studies from the Commission on Federal Paperwork in 1977 through the Grace Commission in 1983 reported on needed improvements in Federal information technology management. In the last few years, the Office of Management and Budget (OMB), General Services Administration (GSA), and various individual agencies have taken numerous management initiatives. And most recently, OMB has given attention to information technology management both as part of overall government management and through specific actions such as the December 1985 circular on "Management of Federal Information Resources."[3]

Nonetheless, OTA identified several further needs for management improvement that appear to be crucial to realizing the full potential of information technology for increasing the efficiency and effectiveness of government. These are discussed briefly below. Many of these needs could be met by the executive branch acting alone. However, Congress can facilitate, encourage, and, where necessary, require these actions.

---

[3] See Office of Management and Budget, *Management of the United States Government Fiscal Year 1986*, and OMB, Circular A-130 on "Management of Federal Information Resources," issued Dec. 12, 1985. Also see OMB, *Management of the United States Government Fiscal Year 1987.*

Strategic Planning

The annual "5-year plans" currently published by OMB (as mandated by the Paperwork Reduction Act) have several significant deficiencies. While the documents are gradually becoming more comprehensive, they are not "plans," and they do not analyze strategies for using information technology to further government missions, either on a governmentwide or individual agency basis. There is no real vision of the future and little discussion of alternative strategies for use and management of information technology.

Despite some more recent efforts to develop thoughtful plans, many agency planning efforts still have some major flaws, including a failure to:

- include strategic as well as operational plans;
- identify innovative opportunities for use of information technology;
- connect planning effectively to implementation;
- involve users, clients, and the interested public in the planning process; and
- explicitly consider the implications of information technology use for protection of information security and privacy.

One vehicle available to Congress for implementing improvements in planning (and other areas) is the Paperwork Reduction Act of 1980, which in part established an information technology management framework for the government. The act is overdue for reauthorization and could be amended to provide a more precise mandate on the strategic planning process and the contents of the 5-year plans.

Information Availability and Data Quality

The weaknesses of the 5-year plans are compounded by serious deficiencies in the scope and quality of information available to Congress, and to the agencies themselves, on key Federal information technology trends and applications. These deficiencies can hamper effective congressional oversight and agency decisionmaking. For this study, in the absence of much needed information, OTA conducted its own survey of Federal agency use of information technology (see app. B for discussion of OTA's Federal Agency Data Request).

A related problem is that the results of General Accounting Office (GAO) audits, computer matches of various Federal record systems, and a variety of other internal and external audits and studies indicate that the quality (completeness and accuracy) of data and records in Federal computerized systems varies widely – from quite good to very poor.[4] Agency (and congressional) decisions based on inaccurate and incomplete information can lead to wasteful or even harmful results or to missed opportunities and failure to identify key problems.

OTA found that there is a need: 1) to specify the types of information that should be reported on a periodic or continuous basis in order to assist both congressional and central agency oversight of Federal information technology, and 2) to strengthen the data quality standards and procedures applicable to computerized Federal systems.

Innovation

Where OTA identified examples of agency innovation—such as the use of electronic mail, videoconferencing, and computer-based decision support—the exchange of this experience and learning with other agencies appeared to be irregular or nonexistent. A common institutional problem is that many agencies either believe that publicizing innovation is "just asking for trouble" or view many innovations as too risky to try at all.

---

[4] For further discussion of Federal record quality, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, 1986 forthcoming.

OTA concluded that actions to encourage agency innovation are needed, such as: establishing informal and formal mechanisms to exchange experiences gained and lessons learned; developing guidelines that provide agencies with room to innovate, but also help detect and resolve emerging issues before they impair the innovation process; and possibly designating a Federal information technology innovation center (or centers).

Procurement

Government information technology procurement is subject to multiple and sometimes conflicting efforts to simultaneously expedite the procurement process (e.g., through GSA's delegation of procurement authority), increase the level of competition (e.g., through congressional enactment of the Competition in Contracting Act), and more clearly demonstrate a significant return on investment in information technology (as now required by OMB).

OTA concluded that it is too early to fully assess the overall impact of these procurement initiatives. However, there is considerable evidence of reduced technological obsolescence over the last 10 years. For example, Federal agencies responding to the OTA survey reported, collectively, a reduction in percentage of Federal mainframe computers over 6 years old from about 60 percent in 1975 to 10 percent in 1984; and an increase in mainframe computers under 3 years old from 30 percent in 1975 to 60 percent in 1984.

Beyond the availability of relatively new equipment, the "success" of procurement is closely tied to the government's ability to plan and define technology needs and to match technology to those needs. It is in this area particularly that problems persist, especially with the larger systems, such as at the Internal Revenue Service and Social Security Administration.[5] There still appears to be a need for: better training of procurement staff, greater senior management involvement in and understanding of the planning and procurement process, improved mechanisms to exchange procurement experience and learning, and possibly a procurement and management troubleshooting team to assist with serious trouble spots.

Information Resources Management (IRM)

In enacting the Paperwork Reduction Act (PRA), Congress directed that each agency designate a high-level official responsible for all aspects of the management of information technology. The information resources management (IRM) concept was intended to bring together previously disparate functions—such as computers, telecommunications, office automation, and the like—and to establish the importance of information as a resource.

OTA found that, while agencies have designated an IRM officer, actual implementation of IRM varies widely and has been only partially or minimally implemented in many agencies. And the Paperwork Reduction Act provides limited or no direct guidance in some key areas such as: the use of information technology to support agency decisionmaking (e.g., computer-based decision support), and public information technology and policy (e.g., electronic databases and electronic dissemination of government information). OTA concluded that there is a need to review progress in PRA implementation since 1980 and clarify the scope of authority and responsibilities intended for IRM officers.

---

[5] OTA is conducting a separate in-depth case study entitled *Federal Government Information Technology: Case Study of the Social Security Administration*, forthcoming in summer/fall 1986.

INFORMATION SYSTEMS SECURITY AND COMPUTER CRIME

Information Systems Security[6]

An important management responsibility is maintaining the security of information systems. If proper security is not maintained, the government cannot assure: 1) the continuity and effectiveness of government operations; 2) the quality (e.g., accuracy and completeness) of information in Federal systems; or 3) control over those types of information (e.g., personal, proprietary, classified) to which access is limited by law or regulation.

The proliferation of microcomputers, continuing rapid increase in mainframe computer systems, large percentage of computerized Federal records (e.g., about 80 percent of Privacy Act records are maintained in fully or partially computerized systems), and growing use of electronic data linkages of all sorts, clearly have increased the difficulty and complexity of protecting government information. Information systems security is now recognized as a serious problem by both civilian and military agencies; the President emphasized information systems security in the September 1984 National Security Decision Directive (NSDD) 145, as has OMB in its December 1985 information management circular.

There is, indeed, cause for concern. OTA found that agencies are often not implementing the measures mandated or suggested under prior policy guidance. For systems that process sensitive but unclassified information, OTA found that:

- about 40 percent of agencies responding have not conducted a risk analysis during the last 5 years, 25 percent do not screen personnel with computer access, and 50 percent do not screen computer applications for sensitivity;
- in addition, about 40 percent of agencies do not use audit software or restrictions on dial-up (remote) access to mainframe computers, and about 80 percent do not use encryption; and
- finally, about 75 percent of agencies responding do not have an explicit security policy for microcomputers, and about 60 percent do not have (and are not developing) contingency plans for use if mainframe computers are disrupted.

The Administration's approach, through NSDD 145, has been to assign a much stronger role to the military and to the National Security Agency (NSA) in particular. While this may well strengthen Federal leadership in information systems security, it also puts the national security community in an unusual, influential if not controlling position on this key aspect of information policy, and could heighten tension between the defense and civilian sectors.

OTA identified several options on information systems security that warrant consideration, including:

- designating a civilian agency to provide information security training and technical support to the civilian sector (similar to NSA's role in the defense sector);
- changing budget procedures to provide more visibility for computer and telecommunications security in agency budget requests (i.e., a security line item); and
- codifying part or all of NSDD 145 into law, clarifying the roles of NSA and civilian agencies so as to remove the possibility that national security agencies might have undue control over civilian agency functions.

Some of these options are reflected, at least in part, in H.R. 2788, the "Computer Security Research and Training Act of 1985," as amended.

Computer Crime

One purpose of good security is, of course, to protect against criminal activity directed towards computer systems and the information they contain. Technical and administrative measures are important parts of good security. But, in addition, criminal laws on computer abuse can provide another disincentive for potential violators and facilitate prosecution when crimes occur.

---

[6] For further discussion of technical security options, see the OTA study on *New Communications Technology: Implications for Privacy and Security* is expected to be completed in winter 1986-87.

Since the 1970s, there has been a growing consensus that existing criminal laws covering the variety of crimes that can be committed with a computer (e.g., fraud, theft, embezzlement, invasion of privacy, trespass) either do not cover some computer abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution. The available evidence suggests that significant losses have occurred. However, the total volume and severity of computer crime is unknown, given a scarcity of reliable information. Nonetheless, the potential (if not current) problem is thought to be so serious that 45 States and, in 1984, the Federal Government, have enacted computer crime laws.

Congress could fine-tune this Federal law (Computer Fraud and Abuse Act of 1984), giving particular attention to the following areas, among others: extending the coverage to private sector computers operating in interstate commerce (currently only Federal computers and those operated by certain financial institutions are covered); refining any overly broad language (e.g., with respect to unintentionally restricting computerized dissemination of or access to public information); and establishing a mandatory computer crime reporting system for Federal agencies (OTA found that only about one-fifth of agencies have a computer crime tracking system or procedures).

OTA found that because many Federal (as well as private) computer systems have computers located in more than one State and/or use data communication networks that routinely cross State lines. State jurisdiction can be hard to establish, given the dynamic nature of computer/communications linkages. On this basis, OTA concluded that some form of interstate Federal computer crime law is warranted.

In general, OTA concluded that effective computer crime legislation needs to balance concerns about the potentially serious nature of such crime with other factors, such as:

- the responsibilities of vendors, owners, and users for the security of their systems;
- the need for effective administrative and technical security measures;
- the need to balance Federal and State roles in the prosecution of computer crime;
- consistency with other aspects of Federal information policy (e.g., Privacy Act, Freedom of Information Act, Omnibus Crime Control Act); and
- consistency with State computer crime laws.

Several of these and other factors are reflected in legislation under active congressional consideration, including: H.R. 1001, "Counterfeit Access Device and Computer Fraud and Abuse Act of 1985"; H.R. 930, "National Computer Systems Protection Act of 1985"; S. 440, "Computer Systems Protection Act of 1985"; S. 610, amendment to Computer Fraud and Abuse Act; and S. 1678 (and H.R. 3381), "Federal Computer Systems Protection Act of 1985."

INFORMATION TECHNOLOGY AND DECISION SUPPORT

One of the less visible but important applications of information technology is to support decisionmaking. In the context of the Federal Government, this could include decisions about governmentwide or agency-specific policies, plans, priorities, budgets, and/or program implementation options. The range of possible applications includes, for example: the use of simple spreadsheet software on microcomputers to help analyze budget options; the running of complex simulation models to better understand the possible impacts of alternative program strategies; the collection and synthesis of information from several electronic databases relevant to the decision at hand; the use of computer graphics to analyze and display key trend and foresight information; and participation in decision conferences where decisionmakers (and staff) use computer and analytical tools to help work through a decision problem.

At the outset of this study, OTA found little systematic information on the use of computer-based decision support in the Federal Government. Computer modeling and electronic databases are not included within the purview of senior IRM officials as their responsibilities are commonly defined. Nor does the language or legislative history of the Paperwork Reduction Act provide guidance as to whether these information technology applications were intended to be included within IRM.

The results of OTA's Federal Agency Data Request provide a profile of the extent and use of these techniques. For example:

- about 60 percent of Federal agency units report at least some use of computer modeling, frequently for decision support (but also for research and scientific purposes), with the number of applications ranging up to 2,000 per agency component; and
- use of computer-based decision analytic techniques appears to have increased dramatically since the advent of microcomputers:
  —about 90 percent of Federal agency units report use of spreadsheet software;
  —about half use quantitative decision techniques (e.g., linear programming, systems analysis, critical path analysis);
  —about one-fourth use forecasting techniques (e.g., regression analysis) and quantitative decision analytic techniques; and
  —about one-twentieth use computer-assisted decision conferences and/or computer conferencing.

Overall, executive branch officials believe these techniques to be very useful, even essential, to agency decisionmaking. However, few can document this claim other than by citing ad hoc examples, because there has been little research on the impact of decision support techniques on agency decisionmaking and little effort to exchange experience among agencies using these techniques.

OTA identified several possible actions that could help to: 1) improve sharing of expertise and learning about computer-based decison support; 2) facilitate congressional and public access where appropriate; 3) enhance understanding of the strengths and limitations, uses and abuses of computer modeling and electronic databases; and 4) improve the government's return on a significant investment. Possible actions that warrant consideration include:

- establishing guidelines or standards for model documentation, verification, and validation (at least for major models);
- establishing directories or indices to major computer models and electronic databases;
- clarifying procedures on congressional and public access to agency computer models and databases;
- conducting further research on the impact of computer-based decision support on agency decisionmaking;
- conducting further testing and development of the decision conference technique;
- developing a formalized foresight capability in major agencies; and
- establishing clear institutional responsibility for some or all of the above, possibly by including decision support as part of information resources management.

A significant, unrealized potential of information technology is to improve the foresight capability of the government. Foresight can be viewed as a component of decision support that involves monitoring and analyzing key longer term trends and their implications for government policies and programs. The combination of computer modeling, electronic data collection, and various decision analytic techniques used in a decision conference format may be an effective technical approach to improve governmentwide foresight capability, when coupled with institutional mechanisms that cut across agency and disciplinary lines. OTA identified several possible actions to help accomplish the latter, ranging from: bringing foresight into the scope of information resources management, to including foresight functions as part of agency decision support centers, to establishing separate foresight offices organized by agency or by subject matter, and to setting up a governmentwide foresight office that would pull together key trends information from the various agencies (as envisioned in S. 1031, the Critical Trends Assessment Act of 1985).

MANAGEMENT OF GOVERNMENT INFORMATION DISSEMINATION

Information technology holds out the promise of faster, cheaper, and more efficient collection (e.g., through computer-aided surveys and document filings), maintenance (e.g., in computerized databases and optical disks), and dissemination of government information (e.g, via electronic mail, interactive data networks, electronic bulletin boards, remote printing-on-demand, and computer tape exchange). OTA's preliminary research in this area suggests that the Federal Government is at or near the threshold of a major shift toward greater use of information technology for managing government information. These technologies could revolutionize the public information functions of the government.

At the same time, because government information is vital to so many users—in and outside of government—and central to numerous public laws and agency missions, the impending shift is raising a wide range of policy issues. The issues are complicated because of perceived tensions between:

- public access and the public's right to know (as embodied in the Freedom of Information Act) and the role of Federal agencies in actively disseminating public information (as mandated in the Public Printing Act and numerous authorizing statutes);
- management efficiency and cost reduction (per OMB circulars, the Deficit Reduction Act, and, to some extent, the Paperwork Reduction Act); and
- particularly for scientific and technical information, national security and foreign trade concerns.

OTA concluded that further research in this area is warranted, but that, ultimately, Congress is likely to be called on to update existing public information laws and address a variety of trends and issues such as:

- reduction of paperwork and publications;
- increasing use of electronic dissemination;
- cost-effectiveness of electronic information options;
- equity of access to government electronic information;
- private sector role in Federal electronic information activities;
- institutional responsibility for government information collection, dissemination, policy, and operations;
- need for a public information index or clearinghouse;
- mechanisms for exchange of learning and innovation;
- Freedom of Information Act implementation;
- electronic recordkeeping and archiving;
- scientific and technical information exchange; and
- other issues such as transborder information flow, depository library system, Federal statistical system, and copyright protection.

INFORMATION TECHNOLOGY AND CONGRESSIONAL OVERSIGHT

This report focuses primarily on executive agency management and use of information technology, and congressional oversight thereof. The trends, issues, and options discussed are properly within the purview of congressional oversight of executive branch programs, activities, and implementation of public laws. However, information technology also has a potential role in the actual conduct of congressional oversight.

Congress as a whole has made great strides over the last 10 to 15 years in using information technology with respect to legislative information retrieval, constituent mail and correspondence management, and some administrative functions. However, the use of information technology for direct support of policymaking and oversight is just beginning.

OTA identified significant unrealized opportunities for congressional use of information technology in conducting oversight, and an apparent lack of clear strategy for such use. A similar situation exists at the State level, based on an OTA review of relevant activities in nine State legislatures (California, New York, Wisconsin, Minnesota, Florida, Washington, Texas, Virginia, and South Dakota).

Four specific opportunities identified by OTA include: 1) direct access by congressional committees and staff to agency electronic files; 2) use of computer-based modeling and decision support; 3) video- and computer-conferencing to augment committee and staff oversight activities; and 4) electronic tracking of agency and executive actions. Congress may wish to plan and conduct a series of pilot tests and demonstrations in each of these areas, in order to more accurately assess the benefits, costs, and problems.

The pilot test approach has worked in the past for new technological applications in Congress. Pilot tests of congressional oversight applications should be useful to help familiarize Members and staff with new applications, identify needs for training, and develop the best match or fit between a particular application and the needs of specific committees, Members, and staff. Also, while Congress has strong constitutional powers to oversee and obtain information from the executive branch, pilot tests would help familiarize the agencies with new applications, identify any needed adjustments, and generally seek approaches that minimize possible concerns about separation of powers and executive privilege.

IN CONCLUSION

OTA's assessment of Federal Government information technology has identified significant progress, problems, and opportunities for improvement in the management and use of this very important technology. Many of the needed improvements can and ultimately would have to be implemented by the executive branch itself. Congress can facilitate and encourage appropriate actions through effective oversight and, where necessary, legislative remedies.

Chapters 2 through 8 of this report provide technical and policy analyses relevant to proposed legislation and policy initiatives on information technology management, including legislation on information systems security and computer crime noted earlier, possible amendments to the Paperwork Reduction Act and Public Printing Act, and governmentwide management initiatives such as the "Government Management Report Act of 1986."

Appendix A to this report briefly discusses other related issues that warrant congressional attention, but are outside the primary focus of this document. Appendix B describes the methodology of and respondents to OTA's Federal Agency Data Request. Appendix C lists the OTA contractor papers relevant to this report. Appendix D lists outside reviewers and contributors.

Chapter 2

Trends in Federal Government Information Technology Management

Contents

Page

Summary 13

Introduction 15

Trends in Information Technology Management 16
  Major Studies and Policy Actions 16
  Information Resources Management 16
  Planning 19
  Procurement 20
  ADP Personnel 24
  Recent Issues 26
  Recent OMB Activities 26

Basic Data on Federal Information Technology Use 28
  Total Expenditures 28
  Medium- and Large-Scale Computers 29
  Microcomputers 29
  Age and Obsolescence of Federal Computers 31
  Length of the Procurement Process 36

Appendix 2A.—Excerpts From Major Studies and Policy Actions in Information Technology Management 37

Tables

Table No. *Page*
2-1. Schedule for GSA Triennial Reviews 18
2-2. Thresholds Below Which Agencies May Procure Information Technology Without a Specific GSA Delegation of Procurement Authority (DPA) (FIRMR Part 201-23) 22
2-3. Average Annual Salaries for Programmers/Programmer Analysts in Private Industry v. Average Annual Salaries for Federal Employees in the GS-334 Series, March 1983 25
2-4. Excerpts From OMB Circular A-130 on Information Technology Management 27
2-5. IDC Projections of Information Technology Sales to the Government 29
2-6. Purchase of Small Computers by Federal Agencies, Fiscal Year 1984 30

Figures

Figure No. *Page*
2-1. The Scope of Information Resources Management 17
2-2. Information Technology Obligations in Current and Constant Dollars 28
2-3. Distribution of ADPE Dollar Value by Reporting Agency 30
2-4. Mainframe Computers in Federal Agencies 31
2-5. Computer Terminals in Federal Agencies 32
2-6. Microcomputers in Federal Agencies 33
2-7. Age of 978 Large- and Medium-Scale Federal Computers 34
2-8. Average Age of Mainframe Computers 35
2-9. Average Procurement Time for Mainframe Computers 37

Chapter 2

Trends in Federal Government Information Technology Management

SUMMARY

The Federal Government has been a major user of information technology since the development of the first generation of digital computers over three decades ago. With each new generation of technology, the government's computer applications have grown and diversified to the point where, today, information technology is vital to the performance of agency missions and the functioning of the government itself.

For the 142 agency components responding to OTA's Federal Agency Data Request, the total number of mainframe computer central processing units more than doubled from about 11,000 in 1980 to about 27,000 in 1985, mainframe computer terminals more than quadrupled from about 36,000 to over 170,000, and microcomputers increased (conservatively) from a few thousand to about 100,000. In sum, the Federal Government has amassed the largest inventory of computer equipment in the world, with a cumulative information technology budget conservatively estimated at over $60 billion (current dollars) for the last five fiscal years.

The management of Federal Government information technology has received high-level congressional and executive branch attention for at least the last two decades, with a new round of studies, reports, and policy initiatives occurring at least every 5 years or so. Management issues involving planning, procurement, security, and the like must be revisited periodically because of the dynamic nature of the technology, among other reasons. Management approaches and policies that worked in the first-generation, centralized computer environment may not be effective or appropriate for the decentralized computer and communication environment that exists today.

Major milestones in Federal information technology management include the:

- 1959 Bureau of the Budget study on the need for automatic data processing (ADP) leadership;
- 1965 Brooks Act (Public Law 89-306) establishing ADP management and procurement policies;
- 1977 Commission on Paperwork report on information resources management (IRM) as a management concept;
- 1979 Office of Management and Budget (OMB) Federal Data Processing Reorganization Project recommending management improvements;
- 1980 Paperwork Reduction Act (Public Law 96-511) establishing centralized information technology management by OMB and agency IRM officers; and
- 1983 Grace Commission report on needed improvements in information technology management and planning.

Major themes cutting across all of these activities include the need for the Federal Government to:

- be vigilant in staying abreast of advancing information technology;
- conduct effective planning to identify opportunities where the technology can help improve government performance;
- ensure that acquisition of the technology is cost-effective and competitive; and
- manage the technology, once acquired, efficiently and with sensitivity to the broader implications (e.g., privacy and security).

The Paperwork Reduction Act of 1980 is particularly significant because it was intended to change information technology management practices in two fundamental ways. First, it was intended to bring together previously disparate functions under one management structure—specifically ADP, telecommunications, office automation, information systems development, data and records management, and, possibly, printing and libraries. Second, the act reorients the focus of information technology management from only hardware and procedures to include the information itself, by establishing the importance of information as a resource and the concept of information resources management (known as IRM).

At the present time, IRM has been only partially implemented by the Federal agencies, and it is unclear whether it will eventually be implemented more completely throughout government. The General Services Administration (GSA) has just begun to carry out triennial reviews of agency IRM plans and activities, and OMB has issued guidelines for long-range information technology planning and a circular on "Management of Federal Information Resources." However, Congress may wish to provide further guidance through amendments to the Paperwork Reduction Act, which has not been updated since 1980 and is overdue for reauthorization. Some possible congressional actions are discussed in the next chapter.

Another recurring issue is information technology procurement. Continuing procurement problems have been the focus of numerous General Accounting Office (GAO) reports and congressional hearings. Government procurement is subject to multiple and possibly conflicting efforts to simultaneously expedite the procurement process (e.g., through GSA's increased delegation of procurement authority), increase the level of competition (e.g., through congressional enactment of the Competition in Contracting Act), and more clearly demonstrate a significant return on investment in information technology (as now required by OMB).

OTA concluded that it is too early to fully assess the overall impact of these procurement initiatives. However, evidence available to OTA suggests that the average age of Federal computers has been decreasing. For example, the results of OTA's Federal Agency Data Request indicate that the percentage of mainframe computers under 3 years old increased from about 30 percent in 1975 to 60 percent in 1984. And the percentage of mainframe computers over 6 years old decreased from about 60 to 10 percent over the same period of time. These results are generally consistent with those of related GSA and National Bureau of Standards studies.

As for the length of the procurement process itself, there are few reliable indicators, and available data are mixed. Responses to the OTA Data Request indicated that the most frequently reported average procurement time for mainframe computers was 1 to 1.5 years in both 1980 and 1984, with relatively few procurements reported to have taken longer than 2.5 years. These time periods may still be excessive, but do not appear to be as lengthy as generally perceived.

While there is a scarcity of reliable data about the government's ADP personnel, a variety of reports and expert opinion suggest that some agencies have serious problems attracting and retaining technical staff. Differing salary levels between the government and the private sector are the most visible cause of such problems, although other contributing factors include the extent to which agency staff can work with up-to-date information technology, and the time it takes to classify and fill positions.

INTRODUCTION

The first part of this chapter provides background on policy issues and trends related to management of Federal information technology, while the second summarizes basic data on the extent of information technology use in government. Later chapters will analyze selected issues and policy options in detail.

It should be emphasized that the management of information and technology is not an end in itself, but rather is a tool to further the various missions of Federal agencies. The most important question is not how well agencies use information technology, but how well they accomplish their missions. OTA's analysis can identify trends, suggest problem areas, and suggest opportunities for further exploitation of information technology tools. Clearly though, each agency must consider these problems and opportunities in the context of its missions and circumstances.

More than three decades have passed since digital computers were first sold commercially. In the 1950s, the Federal Government pioneered many of the early uses of large-scale data processing. The first general-purpose data processing computer, the UNIVAC I, was installed at the Bureau of the Census in 1951. Since that time, tremendous changes have occurred in the technology itself, in government policies, and in organizations that use information technology.

The exponential increase in the power and economy of computers since the 1950s has been well documented.[1] As developments such as the transistor and the integrated circuit have been exploited, the size and cost of computing machines have decreased by several orders of magnitude, and their processing speed and versatility have increased by similar amounts. In addition, microcomputers burst onto the scene in the mid-1970s, changing the nature of the problems for which computers could be used and spreading the control of computing technology into the hands of more people, many without computing backgrounds.

Networking, another major technical trend affecting government information technology management, is closely related to the microcomputer explosion. The past decade has brought substantial improvements in the ease with which information systems can communicate with one another. Packet-switched networks, for example, allow fast and cheap transfer of large amounts of data, usually between larger machines far apart; for smaller machines, the local-area network (LAN) is being used extensively to connect microcomputers and word processors with each other and with larger machines within an office complex. The net effect is that it is much easier for information systems to be decentralized, linked, and interdependent. The management implications of this trend include the technical and administrative challenges of designing distributed computing networks, as well as the security considerations of increased interdependence.[2]

While these trends in computer and telecommunication hardware have received a great deal of attention, there has been an emerging consensus in the past few years that one of the most significant bottlenecks for expanded use of information systems is software, the instructions that make information systems perform useful tasks. The development and maintenance of software systems are still extremely labor-intensive, and both industry and government have begun to focus their management attention on software.[3]

---

[1] This report will not include a primer on trends in computer technology, because such material is readily available. See, for example, U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues*, OTA-CIT-268 (Washington, DC: U.S. Government Printing Office, February 1985); and U.S. Congress, Office of Technology Assessment, *Automation of America's Offices*, OTA-CIT-287 (Washington, DC: U.S. Government Printing Office, December 1985).

[2] See, for example, *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*, A Report of the Panel on Crisis Management of the Georgetown Center for Strategic and International Studies, October 1984. Many of the security issues are discussed in ch. 4.

[3] See, for example, Office of Management and Budget, *Management of the United States Government Fiscal Year 1986*, pp. 47-52.

TRENDS IN INFORMATION TECHNOLOGY MANAGEMENT

Major Studies and Policy Actions

Many common themes can be found in the key reports and policy measures in this area over the past three decades—in particular, the need to use information technology effectively and to control the costs of that use, the need for foresight and planning, and the need for policy leadership and coordination. While there has been progress since the first UNIVAC, the pace of change in information technology, and the evolution of organizations as a result of its use, requires almost continuous attention to issues of planning, effective use, procurement, and policy leadership. Appendix 2A at the end of this chapter presents some excerpts from key studies in this area.

Public Law 89-306 (known as the Brooks Act), enacted in 1965, was the earliest significant congressional action affecting Federal use of information technology. This legislation was prompted by a concern that one supplier (IBM) was dominating Federal automatic data processing, and by GAO reports that agency use of information technology was out of control and that agencies should more often purchase rather than lease equipment.[4] In addition, the Bureau of the Budget (BOB—now OMB) had issued reports and guidelines calling for coordination and "dynamic leadership" in government ADP management, but GAO and others considered BOB's actions to be generally ineffective.[5] Thus Congress, with the leadership of Chairman Jack Brooks (D-Texas) and the House Committee on Government Operations, passed Public Law 89-306, which established central control over ADP in the Federal Government through three agencies: the Bureau of the Budget for policy, the General Services Administration for procurement, and the Department of Commerce/National Bureau of Standards for standards and other technical support.

In the late 1960s and early to mid-1970s, a variety of GAO reports and congressional oversight hearings focused on two topics relevant to information technology management: problems in the implementation of the Brooks Act, and concerns about excessive paperwork imposed by Federal agencies. Two important study groups were established to help grapple with these issues. In 1974, Congress established the Commission on Federal Paperwork, which reported recommendations on decreasing the paperwork burden in 1977; and in 1977, the President created the Federal Data Processing Reorganization Project, which issued a report in April 1979.[6] Both of these reports cited the need for increased coordination of information collection and use in the government, and advocated a more sophisticated, wide-ranging style of management for information technology. Building on these recommendations, Congress passed Public Law 96-511, the Paperwork Reduction Act of 1980. The act joins the two goals—reducing paperwork and improving information and technology management—under the banner of a new concept, information resources management (IRM).

Information Resources Management

The IRM concept is intended to change management practices in two fundamental ways.[7] First, it brings together under one management structure previously disparate functions—specifically ADP, telecommunications, office automation, systems development, data and records management, and in some cases, printing and libraries. The rationale behind this integration is to adopt a management strategy consistent with the convergence of the technologies themselves, as well as a strategy that allows for information functions to be more comprehensively integrated, efficient, and complementary. See figure 2-1 for a graphic representation of this integration.

---

[4] See U.S. General Accounting Office, *Survey of Progress and Trend of Development and Use of Automatic Data Processing in Business and Management Control Systems of the Federal Government as of December 1957*, June 27, 1958; *Review of Automatic Data Processing Developments in the Federal Government*, Dec. 30, 1960; *Study of Financial Advantages of Purchasing Over Leasing of Electronic Data Processing Equipment in the Federal Government*, Mar. 6, 1963; and *Review of Problems Relating to Management and Administration of Electronic Data Processing Systems in the Federal Government*, Apr. 30, 1964.

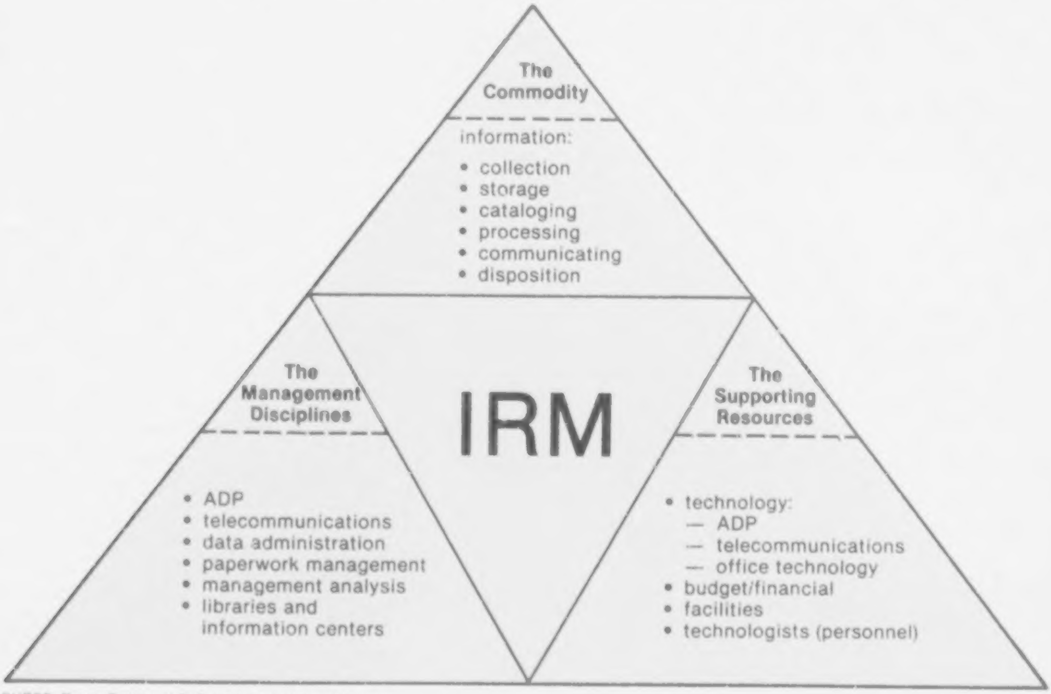
[5] See Bureau of the Budget, "Report of Findings and Recommendations Resulting From the Automatic Data Processing (ADP) Responsibilities Study," September 1958 to June 1959, and "Report to the President on the Management of Automatic Data Processing in the Federal Government," March 1965. For views of BOB's effectiveness, see the legislative history of Public Law 89-306, *U.S. Congressional and Administrative News*, 89th Cong., 1st sess., pp. 3873-3874.

[6] *Information Resources Management, Report of the Commission on Federal Paperwork*, Oct. 3, 1977 (Washington, DC: U.S. Government Printing Office, 1977); and *Information Technology and Governmental Reorganization: Summary of the Federal Data Processing Reorganization Project*, April 1979.

Second, IRM reorients the focus of information systems management from hardware and procedures to the information itself by firmly establishing the importance of information as a resource. Proponents of IRM believe this move is essential as organizations become more information-intensive, because managers must recognize the costs of collecting and keeping information, and they must balance those costs against the value of the information to the organization. One of the chief proponents of the IRM concept writes:

> The time has come to formalize the treatment of information and deal with data as a manageable and budgetable resource, in the same way organizations must deal with human, physical, financial, and natural resources. Dealing with the information explosion piecemeal simply is not working. Information and data costs are increasing, and individuals and organizations are not getting the information they need. Instead, they are being inundated with data to the point where the data cease to be informative. Sophisticated information-handling technologies, including data base management approaches, are leading individ-

Figure 2-1.—The Scope of Information Resources Management


The Commodity
information:
• collection
• storage
• cataloging
• processing
• communicating
• disposition
The Management Disciplines
• ADP
• telecommunications
• data administration
• paperwork management
• management analysis
• libraries and information centers
IRM
The Supporting Resources
• technology:
— ADP
— telecommunications
— office technology
• budget/financial
• facilities
• technologists (personnel)

SOURCE: Roger Cooley, U.S. Department of the Interior

For useful, broad-ranging discussions of information resources management see the report of the Commission on Federal Paperwork, op. cit.; and F. Woody Horton, Jr., and Donald Marchand (eds.), *Information Management in Public Administration* (Arlington, VA: Information Resources Press, 1982).

uals and organizations into a mire of information overload.[8]

In its paperwork-fighting role, the Paperwork Reduction Act mandates the establishment of a Federal Information Locator System so that agencies can determine whether information they want to solicit from the public is already available; it also requires agencies to calculate the number of man-hours required for the public to fill out its various forms, and to compile an "Information Collection Budget" for approval by OMB. In its role as an information resources management directive, the act requires that agencies designate a "senior official" to be responsible for IRM, and that agencies review and evaluate their information management activities. The act established a new Office of Information and Regulatory Affairs within OMB to manage both paperwork reduction and information technology management governmentwide.

One final important consequence of the Paperwork Reduction Act is its mandate for OMB and GSA to develop a "five-year plan for meeting the automatic data processing and telecommunications needs of the Federal Government" (see ch. 3), and for OMB and GSA to review agencies' information management activities at least every 3 years. GSA has just begun to implement a plan for these reviews, and has developed materials to help agencies examine their own IRM activities[9] as a first step toward a GSA/OMB evaluation. If effective, these triennial reviews could help reveal weaknesses and help agencies to share good techniques. See table 2-1 for GSA's schedule for these reviews.

Table 2-1.—Schedule for GSA Triennial Reviews

First-year agencies are those information-intensive agencies (identified by OMB in initial review efforts) with the longest established review programs. Second- and third-year agencies are information-intensive agencies not included in the first year. Agencies have been listed if they are large enough to have an established IRM organization. All other agencies are also included in the third year.

Beginning in FY 86, and every third year thereafter

Year 1 agencies:

Department of Agriculture
Department of Commerce
Department of Education
Department of Energy
General Services Administration
Department of Health and Human Services
Department of the Interior
Department of Justice
Department of Labor
Department of Transportation
Veterans Administration

Beginning in FY 87, and every third year thereafter

Year 2 agencies:

Consumer Product Safety Commission
Environmental Protection Agency
Federal Energy Regulatory Commission
Federal Trade Commission
Department of Housing and Urban Development
Interstate Commerce Commission
National Aeronautics and Space Administration
National Science Foundation
Office of Personnel Management
Department of State
Department of the Treasury

Beginning in FY 88, and every third year thereafter

Year 3 agencies:

Action
Commodity Futures Trading Commission
Department of Defense
Department of the Air Force
Department of the Army
Department of the Navy
Federal Communications Commission
Federal Emergency Management Agency
Federal Reserve System
Nuclear Regulatory Commission
Securities and Exchange Commission
Selective Service System

SOURCE: General Services Administration, *IRM Review Handbook*.

Based on OTA's workshops and other contacts with Federal agency officials, it appears that many agency staff seem to view IRM in one of two ways:

1. as an umbrella term, used in a wide variety of discussions about ways to improve use of information technology in government, in many cases similar to the way the term ADP (automatic data processing) is used; or
2. as an interesting and worthwhile concept, but much too broad to have substantial impact on down-to-earth problems.[10]

---

[8] F. Woody Horton, Jr., "Needed: A New Doctrine for Information Resources Management," p. 45, in Horton and Marchand, op. cit.

[9] General Services Administration, *IRM Review Handbook*, FIRMR 201-19, fiscal year 1985. The handbook contains a set of provocative questions for each aspect of an agency's IRM activities that are particularly helpful in assessing information technology management practices.

[10] This observation is based on OTA work sessions with several dozen executive agency officials on Oct. 25, Oct. 31, and Nov. 2, 1984; several other OTA events that included exten-

On the other hand, to the extent that IRM serves as a vehicle for coordinating and addressing those down-to-earth problems—essentially planning, procurement, personnel, and prestige within the agency—it is viewed as a useful organizational approach. As is probably true with any new (or relatively new) concept, as the concept moves from its guiding principles through the various stages of implementation, the broad philosophy becomes more and more distant. Too, agency staff must cope with the realities of resource constraints, bureaucratic inertia, and internal and external politics. Essentially, at the operating level agency staffers appear to draw from IRM concepts and techniques that which they find useful. It is unclear at this early stage of implementation whether this partial implementation will continue to be the case, or whether IRM will eventually be implemented more completely throughout government.

One of the difficulties in determining the effectiveness of the IRM concept is the wide variation of problems, missions, and management styles in the Federal Government. As an OMB report notes:

> . . . It is critical to keep in mind, however, that information resources management is simply a means to perform agency missions and is not an end in and of itself. As such, its use varies across agencies. It is a tool that managers use to achieve objectives that often have little or nothing to do with information resources management. It is successful if it enables managers to achieve those objectives cost effectively and it is unsuccessful if it does not.[11]

Planning

The need for information technology planning has been apparent almost since the government began using information technology. For example, a 1960 GAO report,

> . . . call(ed) attention to the need for more positive central planning of a long-range nature within the executive branch of the government to promote the maximum degree of efficiency, economy, and effectiveness in the administration and management of costly automatic data processing facilities.[12]

The Paperwork Reduction Act of 1980, as noted above, requires OMB and GSA to develop a 5-year plan for Federal Government information technology. The act does not assign specific planning tasks to agencies themselves, although it does include planning under the general rubric of the duties of the agencies' information resource managers.

While the Federal Government has begun to address the need for planning for information systems, the private sector has been actively pursuing such planning as well. Businesses have also become more dependent on information technology, and information technology management has gradually become more visible in corporate organizations. In fact, much of the business oriented literature on information technology planning focuses on the use of computers not only to keep track of the business, but also to provide a competitive edge—for example, by enhancing the firm's flexibility and responsiveness, or by helping corporate executives focus only on information that is critical for competitiveness.[13]

Despite what seems to have been a groundswell of support for information technology

---

sive participation by executive agency staff; OTA staff site visits to agencies; OTA staff attendance at professional meetings and seminars; and personal contacts. See also Robert Head, "IRM and Reality," *Government Data Systems*, May/June, 1984, pp. 45-46.

[11] Office of Management and Budget, General Services Administration, and Department of Commerce/National Bureau of Standards, *A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, June 1985, p. 17.

[12] U.S. General Accounting Office, *Review of Automatic Data Processing Developments in the Federal Government*, December 1960, p. 1.

[13] See, for example, the work of the Center for Information Systems Research at the Sloan School of Management, Massachusetts Institute of Technology. Highlights include, John Rockart, "Chief Executives Define Their Own Data Needs," *Harvard Business Review*, March-April 1979; John Rockart and A.D. Crescenzi, "Engaging Top Management in Information Systems Planning and Development: A Case Study," Paper # 115 in the Center's working paper series, July 1984.

planning, there continues to be a consensus that most Federal agencies do not plan as much or as effectively as they should, and that this is partly responsible for many problems, and for their failure to use information systems effectively. Clearly, this situation is also closely tied to weaknesses in many agencies' overall planning.[14]

In the past few years, the demands for effective planning for Federal information technology seem to have reached a crescendo. The Office of Management and Budget, the General Services Administration, and others have strengthened their policy guidelines and issued a variety of handbooks to help agencies plan effectively for information technology use.[15] (See ch. 3 for further discussion of information technology planning.)

Procurement

As noted above, the procurement process has been a subject of much controversy since the 1960s, and concerns about the way agencies acquired and managed their computers were the prime motivating force behind the Brooks Act of 1965. Since the act was passed, the Federal Government's strategies for acquiring and managing information technology have been in a state of near-constant flux. Congress, and especially the House Committee on Government Operations, has continued to express concern, particularly about the use of noncompetitive or "sole source" procurement procedures to obtain information technology. A 1976 oversight report by the House Committee on Government Operations concluded that noncompetitive procurements were caused largely by a lack of adequate justifications for ADP acquisition, inadequate long-range planning, insufficient development and use of standards and high-level languages, failure of agencies to use existing ADP resources efficiently, and the infrequent use of functional specifications in procurement requests (rather than more restrictive technical specifications).[16]

Essentially, the key aspect of information technology that makes a fair and competitive procurement even more difficult than other procurements is the problem of compatibility between old and new systems. In most cases, new ADP technology will require modifications in system configuration, telecommunications, and especially software, that can become intricate, lengthy, and difficult to resolve. Hence, beyond other considerations that may push Federal managers toward limiting competition in their procurements—e.g., complex procurement processes, inadequate planning, personal preferences, or even corruption—managers in both the public and private sectors tend to prefer new technology that is as compatible as possible with existing technology to minimize disruption in the conversion process.

In general, the level of frustration in implementing the Brooks Act has been high, not only for Congress, but also for the central management agencies and the mission agencies. As one analyst observed:

> Each step in developing the law and policy for ADP acquisition and management has been tested (by congressional staff, OMB, GSA, GAO, and by affected agencies) against

---

[14] This consensus can be observed throughout congressional hearings and oversight, in many (perhaps most) GAO reports (e.g., *Continued Use of Costly, Outmoded Computers in Federal Agencies Can Be Avoided*, Dec. 15, 1980; *Inadequacies in Data Processing Planning in the Department of Commerce*, May 1, 1978; *Strong Centralized Management Needed in Computer-Based Information Systems*, May 22, 1978; *GSA's Telecommunications Procurement Program Requires Comprehensive Planning and Management*, June 11, 1984), and in a variety of other fora (see, e.g., Robert Head, "Federal Information Systems Management: Issues and New Directions," a staff paper published by The Brookings Institution, 1982).

[15] These include volume 1 of OMB's *Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, April 1984, which includes a primer on information technology planning and several examples of specific agencies' planning processes; OMB's Bulletin 85-12 (Mar. 29, 1985), which provides guidance to agencies on planning and requires them to submit planning documentation to OMB; GAO's *Questions Designed To Aid Managers and Auditors in Assessing the ADP Planning Process*, Sept. 30, 1982; and GSA's *IRM Review Handbook*, fiscal year 1985, and *Strategic Information Resources Management Planning Handbook*, February 1985. GSA has also begun a Federal IRM Planning Support Program to provide limited assistance to agencies in their planning process.

[16] House Committee on Government Operations, Report 94-1746, *Administration of Public Law 89-306, Procurement of ADP Resources by the Federal Government*, Oct. 1, 1976, p. 3.

> its assumed ability to produce the objectives sought. Each applicable policy document (e.g., Public Law 89-306, GSA directives, NBS standards, and OMB circulars) has met the test of logic. Yet numerous GAO reports and congressional committee hearings support the conclusion that the end results have been astonishingly ineffective. In short, the law *meets all rational tests* and *has not achieved the expected gains* in economy and efficiency.[17]

In 1984, in part as a result of some of these frustrations, Congress passed the Competition in Contracting Act. The act considerably strengthens the regulations governing all procurements, requires each agency to designate a "competition advocate," and requires full and open competition in as many procurements as possible. Significantly, the new act considers both "competitive negotiation" and purchases from negotiated schedule contracts[18] as full and open competition, allowing contracting officers some welcomed options in an otherwise stringent law. The act prescribes certain exceptions that justify noncompetitive procurements. These are:

- the property or services are available from only one responsible source;
- there is "unusual and compelling urgency";
- it is desirable to award the contract to a particular source in order to maintain the existence of a supplier or to meet the terms of an international agreement;
- noncompetitive procurement is specifically authorized by statute;
- the disclosure of the agency's needs would compromise national security; and
- the head of the agency determines that it is "necessary in the public interest" to use noncompetitive procedures, and notifies Congress in writing 30 days before award of the contract.

In addition, the act sets up a special procedure to resolve disputes between agencies and vendors of ADP equipment. Under this procedure, the Board of Contract Appeals at GSA is given authority to suspend procurement authority if necessary, and to issue a decision on the protest within 45 working days after the protest is filed.[19]

The Competition in Contracting Act is also having a direct and immediate effect on GSA, where an effort is under way to rewrite the procurement regulations to conform with the act. In addition, GSA has been attempting for several years to simplify procurement procedures. For example, GSA recently combined its primary guidance on information technology procurement into a 100-page document, the Federal Information Resources Management Regulation. Also, in recent modifications of procurement guidelines, GSA has continued a key trend to decentralize procurement authority to the agencies and try to minimize GSA's centralized procurement role.

Agencies have blanket authority to procure ADP hardware without GSA approval when the cost is below certain thresholds (see table 2-2). GSA evaluates the procurement practices of agencies and occasionally raises or lowers their thresholds for delegation of procurement authority, based on performance in executing effective procurements and maximizing competition. Finally, in late 1985, GSA announced

---

[17] Paul Richard Werling, *Alternative Models of Organizational Reality: The Case of Public Law 89-306*, doctoral dissertation for the University of Southern California, August 1983, p. 9.

[18] Competitive negotiation allows contracting officers to discuss the terms and conditions of a contract with bidders, and to consider factors other than price in the award of the contract. It is in contrast to "sealed bids," in which there is generally no discussion and the contract is awarded based on price alone. Purchases from "schedule contracts" are for lower dollar value items for which GSA has negotiated a government-wide price with the vendor. These vendors and prices are usually found in GSA's Schedule C.

[19] The act also provides for a general procurement protest system that can be used for all contracts, although vendors cannot protest using both systems. It is this more general protest system that has been so controversial since the act was passed. It gives the Comptroller General authority to decide protests (normally within 90 working days of filing). OMB and the Attorney General argued that giving the Comptroller General such authority was a violation of Constitutional separation of powers because GAO is an arm of the legislative branch. Attorney General Meese initially instructed executive agencies not to comply with the act, but backed down after a U.S. District Court decision upheld the act, and a congressional committee voted to cut off procurement funds for the executive branch if they did not comply. The court decision is being appealed to the third U.S. Circuit Court of Appeals. (Myron Struck, "Meese Averts Showdown on GAO Contract Power," *Washington Post*, June 5, 1985.)

Table 2-2.—Thresholds Below Which Agencies May Procure Information Technology Without a Specific GSA Delegation of Procurement Authority (DPA) (FIRMR Part 201-23)

	Competitive	Sole source	Schedule
ADPE	$2.5 million (purchase price) $1.0 million (annual rental)	$250,000 (purchase price) $100,000 (annual rental)	$300,000 (purchase price) (whether leased or purchased)
Software	$1 million (total procurement)	$100,000 (total procurement)	Maximum order limitation[a]
ADPE maintenance	$1 million (annual charges)	$100,000 (annual charges)	Maximum order limitation[a]
Commercial ADP services	$2 million (annual charges)	$200,000 (annual charges)	$2 million (if competitive) $200,000 (if sole source)
ADP support services	—Authority is granted for all acquisition actions—		

[a] Varies according to the particular contract or product.

NOTE: DPA thresholds were increased under FPR Temporary Regulation 71 to these levels and were permanently codified via FIRMR Amendment 4, effective Oct. 1, 1985.

ADPE = Automatic Data Processing Equipment.

SOURCE: General Services Administration.

a new program, "Go for 12," whose goal is to help other agencies get computers delivered within 12 months after budget approval. GSA is developing the details of the program in cooperation with selected Federal agencies.[20]

Agencies can now obtain small computer systems with virtually no restrictions except normal internal review of purchases. The procedures for acquiring equipment costing less than $25,000 have been streamlined. And GSA has opened two new routes for purchase of such smaller systems: a retail store operated under contract (Office Technology Plus), and a centrally negotiated "schedule" of prices with a wide range of vendors. Responding to concerns about relatively uncontrolled purchase of personal computers, GSA has also issued some (nonbinding) guidance to agencies on such procurements.[21]

OMB has also made significant changes in guidance regarding information technology procurement. In a report submitted with the fiscal year 1986 budget, OMB required agencies to document a 10 percent return on their information technology investments, implement standards permitting communication between systems, encourage the procurement of commercially available software instead of custom-written software, and reduce their software maintenance costs by 25 percent, and by 5,000 FTEs, over fiscal years 1986 to 1988.[22] Though the effectiveness of these measures remains to be seen, the refocusing of some attention to software, rather than hardware, appears well advised. As OMB noted in its report, software costs amounted to less than 20 percent of Federal computer expenditures in 1965, but represent 60 percent of expenditures today. Yet, the government still develops custom software for 90 percent of its applications, which results in redundancy of software development projects, difficulties in system conversions and upgrades, and added expense. However, in some cases the nature and size of Federal applications may require custom software. For example, while "off-the-shelf" software is likely to be useful for common administrative applications such as budgeting or personnel management, it is less likely to be useful for management of immense databases (e.g., Social Security Administration or Internal Revenue Service).

The Federal Government's information technology managers have been arguing for at least a decade that the procurement process is hopelessly complex and is blocking attempts to use information technology effectively and innovatively.[23] As far as OTA can discern, this group is just as vehement on this point as ever.[24] Nevertheless, a small and perhaps growing group of officials say that with some resourcefulness it is indeed possible to get through the apparent maze of processes and regulations and conduct successful and competitive procurements.[25]

---

[20] General Services Administration, "Draft Executive Summary of the Go For 12 Program," February 1986.

[21] *Managing End User Computing in the Federal Government*, June 1983; and *End User's Guide to Buying Small Computers*, August 1984.

[22] OMB, *Management of the United States Government, Fiscal Year 1986.*

[23] See, for example, Robert Head, *Federal Information Systems Management: Issues and New Directions*, op. cit.

In its December 1985 Policy Circular, "Management of Federal Information Resources" (discussed in more detail below), OMB's endorsement of competitive procurement is less wholehearted than that of Congress. An appendix to the circular states:

> While competitive procurement is generally to be valued, its costs should be taken into account, including the cost to program effectiveness of unnecessarily lengthy procurement processes. Other conditions, such as the need for compatibility, may also be legitimate limitations on the competitive process.[26]

Federal managers would support this statement and, indeed, the lifecycle costs of information systems to the government include the costs of procurement. However, the spirit of this statement reflects the divergence in views between Federal managers, who would prefer to err on the side of effectiveness even if that means less competition, and congressional oversight committees such as House Government Operations, whose preference (expressed both in legislation and in hearings) has been for competitive procurements in the absence of extremely compelling circumstances indicating otherwise.

Other recent administrative changes in the process also seem to be pulling procurement in different directions. GSA is attempting to give agencies greater autonomy in procurements and simplify the regulations, while at the same time OMB is requiring demonstrated returns on investment. Most executive branch officials seem to see the Competition in Contracting Act as likely to lengthen and complicate many procurements, because of the ease with which vendors can file protests and delay the process, and because it is unclear under the new law to what extent agencies can conduct "compatibility-limited" procurements (that is, requiring that vendors' proposals only include products compatible with a certain kind of system or architecture) and still be considered fully competitive.[27]

Yet, many of the delays in procurement processes may be due to procedures within the agencies, as well as to regulations imposed on the agencies by GSA, OMB, or Congress. One participant at an OTA meeting, for example, said that he had been trying to procure 40,000 feet of coaxial cable—presumably a simpler procurement than, for example, a large computer system—and that after 15 months it was still not clear when the paperwork would clear his internal bureaucracy. Experienced observers of Federal procurement report that procurement offices are frequently understaffed and besieged by changes in regulations and in technology. In addition, the procurement officers themselves often believe that delay is desirable, either because the time may allow a better deal for the government, or because their jobs make them exceptionally vulnerable to criticism for a mistake in procurement procedures.[28]

A 1981 study on acquisition of ADP equipment for the Air Force may be somewhat indicative of the problems in government ADP procurement, although the Defense Department has many more layers of hierarchy than other, smaller agencies. The report's findings indicated that the procurement process is unnecessarily lengthy (the Air Force takes an average of three times as long as industry to procure ADP equipment, according to the report), resulting in sacrifices in acquisition cost and capabilities; and that the agency was focusing on a misplaced notion of short-term economy and efficiency (i.e., spending the least money to purchase the machine) at the expense of achieving its mission effectively.[29]

---

[24] The impression that Federal managers' dissatisfaction with the procurement process has not eased significantly comes from OTA's meetings with Federal agency representatives, Oct. 25, Oct. 31, and Nov. 2, 1984; and from a variety of conferences and other personal contacts.

[25] See, for example, Frank Guglielmo, Acting Director, Computer Technology and Telecommunications Staff, Office of Information Technology, Department of Justice, "Streamlining Acquisition," address to Government Computer Expo, Washington, DC, June 13, 1985.

[26] OMB Circular A-130, p. IV-13.

[27] Francis McDonough, General Services Administration, letter to OTA, September 1985.

[28] OTA work session on information technology management, planning, and procurement, June 26, 1985.

ADP Personnel

The availability of staff to manage and operate Federal information technology is another ongoing problem in Federal information technology management. Although there is a widespread perception among Federal managers that the government cannot compete effectively in hiring and retaining computer staff,[30] there is only sketchy and largely anecdotal evidence to support this assertion and identify the magnitude of the problem. Further, agency personnel problems differ greatly because of variations in management and personnel practices, and in levels of sophistication in information technology use.

The perceptions of potential employees can be a significant factor in attracting them to an agency. For example, the extent to which an agency uses state-of-the-art technology is an important attraction for ADP staff, and some agencies, such as the National Aeronautics and Space Administration (NASA), report that their image as a leader in technology continues to help them attract good technical staff.[31] In other cases, reports of budget cuts or hiring freezes, in addition to a perception that many Federal agencies use obsolete ADP equipment (a perception that may be increasingly inaccurate, as noted below), tend to make recruiting and retention more difficult.

One of the key arguments is that computer specialists can command higher salaries in the private sector, and thus are not attracted to lower paying jobs in the Federal Government.

An Office of Personnel Management (OPM) study provides some support for this argument, indicating that pay differences are greatest at entry level, where Federal GS-5 salaries are 24.2 percent below those in the private sector. This difference drops to 12.3 percent at GS-12 (see table 2-3).[32] While the Federal Government is by law supposed to pay its employees salaries comparable to average salaries in the private sector, the pay increases in the last few years have lagged behind the government's analysis of what is necessary to maintain comparability.

Further, comparisons between Federal and private sector pay are not entirely straightforward because of differences in position definitions, fringe benefits, and regional costs of living.[33] Other indicators do support pay-related personnel problems in this area, however. A study conducted by the Dallas region of OPM indicated that:

- GS-334 (the designation for Federal computer jobs; see footnote 32) positions have a higher vacancy rate than other comparable government jobs in the region (8.4 v. 5.5 percent as of April 1984);
- positions at the GS-5, GS-7, and GS-14 levels have even higher vacancy rates (23.1, 14.5, and 13.2 percent, respectively);
- GS-334 jobs take longer to fill than comparable jobs (a median of 83 days vacant v. 60 for other jobs); and
- turnover rates are particularly high at the GS-5, GS-7, and GS-14 levels.[34]

---

[29] Booz-Allen & Hamilton, Inc., *Defense ADP Acquisition Study*, prepared for U.S. Air Force ADP Acquisition Improvement Group and Defense Systems Management College, Nov. 30, 1981.

[30] See, for example, President's Private Sector Survey on Cost Control (known as the Grace Commission), *Report on Automated Data Processing/Office Automation*, spring-fall 1983, pp. 85-103; and S.M. Menke, "Budget Blues: Agencies Losing ADPers," *Government Computer News*, Mar. 8, 1985, p. 1.

[31] Charles Mason, National Aeronautics and Space Administration, personal communication, January 1986.

[32] Office of Personnel Management, *Computer Specialist (GS-334) Classification Study: Agency Compliance and Evaluation*, February 1984. To the extent that there is information available about Federal ADP personnel, it tends to focus on the GS-334 series, which includes programmers, programmer analysts, systems programmers, systems analysts, equipment analysts, and computer specialists. There is considerably less information available about computer scientists, or other Federal technical staff who work with computers but whose classification is not strictly computer-related.

[33] Grace Commission, op. cit.

[34] Dallas Region, Office of Personnel Management, "Report of Regional Probe: Recruitment and Retention of Computer Specialists," August 1984.

Table 2-3.—Average Annual Salaries for Programmers/Programmer Analysts in Private Industry v. Average Annual Salaries for Federal Employees in the GS-334 Series, March 1983

BLS level	GS grade	BLS[a] average	Federal[b] average	Difference Federal v. BLS	1983 GS range		1984 GS range	
					Minimum	Maximum	Minimum	Maximum
I	5	19,777	14,998	–24.2%	13,369	17,383	13,837	17,986
II	7	22,148	17,640	–20.4%	16,559	21,527	17,138	22,277
III	9	26,224	21,553	–17.8%	20,256	26,331	20,965	27,256
IV	11	31,446	27,155	–13.6%	24,508	31,861	25,366	32,980
V	12	38,125	33,448	–12.3%	29,374	38,185	30,402	39,519

SOURCES: Office of Personnel Management, using data from:
[a]National Survey of Professional, Administrative, Technical, and Clerical Pay, March 1983 (BLS Bulletin 2181 dated September 1983).
[b]PATCO Report, March 1983 (OPM, Office of Workforce Information).

Virtually all of the data on ADP personnel are preliminary or based on limited samples. Until more authoritative studies are done, it is difficult to assess the magnitude of the problem and determine appropriate policy steps.[35]

A final issue in assessing ADP personnel is the classification system used by the Federal Government to assign jobs to position levels based on the responsibilities and skills needed in the job. Preliminary findings from a study begun by OPM show that 28.5 percent of Federal employees in the GS-334 series are overgraded (that is, their grades are higher than their responsibilities and skills indicate). In the civilian agencies, this figure rose to 44.7 percent. By comparison, a 1981 study found an overgrading rate of 14.3 percent in white-collar government jobs as a whole.[36] It is not clear to what extent overgrading is a result of agency attempts to make pay more competitive, or other factors such as inappropriate use of the classification schemes. In any case, the classification system—and in particular, the Federal practice of reclassifying most positions when they fall vacant—can exacerbate other recruitment problems because it can extend the time necessary to fill a position.

A variety of solutions have been tried or proposed to ease ADP personnel problems. One agency, for example, provides a training program for persons hired in the GS-334 series. The program recruits graduates with advanced degrees, little computer experience, and good academic records to enter a 2- to 3-year program. As they are being trained to become computer specialists, they are able to enjoy pay raises and prove themselves in the field. The disadvantages of this training program are that it is expensive, not all recruits become skilled in the use of computers, and some may leave the government after training.[37]

The Federal Employees Recruitment and Retention Improvements Act of 1985 (H.R. 2836, sponsored by Representative Frank Wolf, and S. 1327, sponsored by Senator Paul Trible) has been proposed to exempt computer specialists from pay freezes in order to retain employees in computer-related fields, and to reduce the lag between the time a position becomes available and the time a candidate is approved by OPM for hire. Another draft bill circulating within OPM and the Office of Science and Technology Policy, the Federal Science and Technology Revitalization Act, is said to propose allowing public sector wages to match those of the private sector, and to provide for merit raises and the abolishment of automatic raises in enumerated science and technology jobs.[38]

Finally, the Grace Commission's report suggested that:

- OPM and GSA should collaborate on

---

[35] The Office of Personnel Management has been working on a more authoritative and in-depth study of ADP personnel, but completion and release of the report are indefinite. (Tony Ingrassia, OPM, personal communication, January 1986.)

[36] OPM, *Computer Specialist Classification Study*, op. cit.

[37] Carl Lowe, Bureau of Labor Statistics, personal communication, January 1986.

[38] Eric Fredell, "ADPer Shortage a Myth? Some May Escape Freeze," *Government Computer News*, Oct. 11, 1985, p. 1; and Eric Fredell, "Reagan Eyes Higher Tech Pay: Bill Designed to Support Recruitment, Retention," *Government Computer News*, February 1985, p. 1.

ways to streamline the classification system;

- agencies should find ways to speed the hiring cycle, for example by reclassifying positions on a fixed schedule instead of when vacated;
- the government should investigate ways to make the classification system more flexible; and
- the agencies should increase the use of cash incentives to reward performance for ADP personnel.

GAO concurred with the essence of these recommendations.[39]

Recent Issues

Since the Paperwork Reduction Act was passed, debate and controversy continue around the issues of information technology management:

- The Senate Governmental Affairs Committee and the House Government Operations Committee have held hearings on progress in implementing the Paperwork Reduction Act, and both Representative Jack Brooks and Senator John Danforth introduced amendments to the act in the 98th Congress that specified further paperwork reductions and clarify and enhance other portions of the act.[40] The amendments passed the full House and the Senate Governmental Affairs Committee, but were not taken up in the full Senate. As of January 1986, similar legislation had not been introduced in the 99th Congress, although Senator Dale Bumpers has proposed an amendment to the Paperwork Reduction Act that would further reduce the paperwork burden on small businesses.
- The President's Private Sector Survey on Cost Control, also known as the Grace Commission, issued a report calling for a variety of changes in Federal ADP management, including steps that would enhance central leadership of information technology use, and steps that would provide more autonomy for agencies in their use of ADP.[41]
- The General Accounting Office has evaluated progress in implementing the Paperwork Reduction Act, noting that although OMB has reportedly achieved the paperwork reduction goals, many other aspects of the act still need a great deal of attention.[42]

Recent OMB Activities

Much of OMB's activity in the first few years of implementation of the Paperwork Reduction Act has concerned establishment and clarification of paperwork reduction procedures. In the area of information and technology management more broadly, there are two significant sets of actions that OMB has recently undertaken. First, OMB has begun to set guidelines and incentives for agencies to conduct long-range planning. These topics are discussed in more detail in chapter 3. Second, in December 1985, OMB issued a circular, "Management of Federal Information Resources," which supersedes several other circulars and essentially provides guidance for agencies in adopting the IRM approach mandated by the Paperwork Reduction Act. It is essentially OMB's first major attempt to take a leadership role in IRM policy.

---

[39] Grace Commission, op. cit.; and General Accounting Office, *Compendium of GAO's Views on the Cost Savings Proposals of the Grace Commission*, Feb. 19, 1985, p. 1024.

[40] U.S. Senate, Subcommittee on Information Management and Regulatory Affairs, hearings on the Paperwork Reduction Act Amendments of 1984, Apr. 4, 1984; U.S. Senate, Committee on Governmental Affairs, Report 98-576 to accompany S. 2433, the Paperwork Reduction Act Amendments of 1984; House Committee on Government Operations, Subcommittee on Government Information, hearings on the Paperwork Reduction Act Amendments of 1983 (H.R. 2718), Apr. 27, 1983. In the 99th Congress, the Senate Governmental Affairs Subcommittee on Intergovernmental Relations also held hearings on implementation of the Paperwork Reduction Act, Jan. 28, 1986.

[41] President's Private Sector Survey on Cost Control, *Report on Automated Data Processing/Office Automation*, spring-fall 1983.

[42] *Implementing the Paperwork Reduction Act: Some Progress, But Many Problems Remain*, GGD 83-85, Apr. 20, 1983.

Table 2-4.—Excerpts From OMB Circular A-130 on Information Technology Management

Information systems and information technology management

Agencies shall:

1. Establish multiyear strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the bases for their budget requests.
2. Establish systems of management control that document the requirements that each major information system is intended to serve; and provide for periodic review of those requirements over the life of the system in order to determine whether the requirements continue to exist and the system continues to meet the purposes for which it was developed.
3. Make the official whose program and information system supports responsible and accountable for the products of that system.
4. Meet information processing needs through interagency sharing and from commercial sources, when it is cost-effective, before acquiring new information processing capacity.
5. Share available information processing capacity with other agencies to the extent practicable and legally permissible.
6. Acquire information technology in a competitive manner that minimizes total lifecycle costs.
7. Ensure that existing and planned major information systems do not unnecessarily duplicate information systems available from other agencies or from the private sector.
8. Acquire off-the-shelf software from commercial sources, unless the cost-effectiveness of developing custom software is clear and has been documented.
9. Acquire or develop information systems in a manner that facilitates necessary compatibility.
10. Assure that information systems operate effectively and accurately.
11. Establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems.
12. Assure that only authorized personnel have access to information systems.
13. Plan to provide information systems with reasonable continuity of support should their normal operations be disrupted in an emergency.
14. Use Federal Information Processing and Telecommunications Standards except where it can be demonstrated that the costs of using a standard exceed the benefit or the standard will impede the agency in accomplishing its mission.
15. Not require program managers to use specific information technology facilities or services unless it is clear and is convincingly documented, subject to periodic review, that such use is the most cost-effective method for meeting program requirements.
16. Account for the full costs of operating information technology facilities and recover such costs from government users.
17. Not prescribe Federal information system requirements that unduly restrict the prerogatives of heads of State and local government units.
18. Seek opportunities to improve the operation of government programs or to realize savings for the government and the public through the application of up-to-date information technology to government information activities.

SOURCE: Office of Management and Budget, "Management of Federal Information Resources," OMB Circular A-130, Dec. 12, 1985, Sec. 8b.

Table 2-4 displays some of the key points of the circular that affect information technology management. Essentially, it sets forth in one place a collection of extremely desirable goals for Federal information technology management. According to the circular, agencies should, for example, use strategic planning, procure information systems in a timely fashion (with the assistance of GSA), control and review major information systems, share resources with other agencies, not duplicate software or resources available commercially, and operate information systems effectively and securely. The fact that these goals are all stated clearly and in one place is an accomplishment; however, few of these goals represent significant changes from previous OMB and congressional policies, and in only a few cases does the circular provide enough detail to be of substantial help to agencies in achieving the goals.[43] Thus, while the circular is a key organizing document for policy, it was intended to be a very general policy statement and thus does not, in itself, make much progress in addressing problems of information technology management.

---

[43] The only areas that are treated in some detail in the circular are dissemination of information, which is discussed in ch. 7 of this report; the treatment of records about individuals, which is discussed in OTA's report on *Electronic Record Systems and Individual Privacy* (forthcoming); and to a lesser extent, information systems security, which is discussed in ch. 4 of this report.

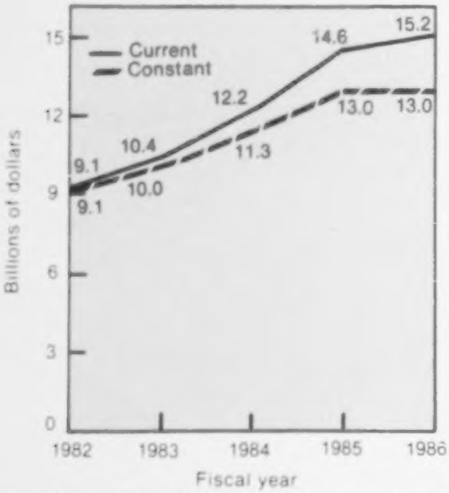
BASIC DATA ON FEDERAL INFORMATION TECHNOLOGY USE

Total Expenditures

As noted in figure 2-2, OMB expects expenditures for information technology to rise from $9.1 billion in fiscal year 1982 to $15.2 billion in fiscal year 1986. This amounts to a 17 percent annual growth rate between fiscal years 1982 and 1985, and a 4 percent growth between fiscal years 1985 and 1986; adjusted for inflation, the growth rate for fiscal years 1982 to 1985 is 13 percent annually, while fiscal years 1985 to 1986 is constant after inflation.[44] A growth rate higher than general government spending is expected to continue, despite austerity measures throughout government. As shown in table 2-5, an International Data Corp. forecast expects sales to the Federal Government to reach $23.8 billion per year by 1988.[45] Although the Gramm-Rudman-Hollings deficit reduction measures are sure to affect spending for information technology, the magnitude of those effects is difficult to foresee. Determining the fiscal year 1987 budget for information technology requires a cross-agency analysis that OMB will not release until spring 1986. Nevertheless, OMB staff expect that cuts in information technology budgets will not be as severe as cuts in other areas, because of the labor-saving and efficiency-increasing capabilities of the technology.[46]

The scope and accuracy of these data should be viewed with some caveats. The numbers are provided to OMB in agencies' annual budget submissions, and they exclude computers and telecommunications used, for example, in classified activities, in weapons systems, in space exploration systems, or in the legislative or judicial branch. In addition, GAO has criticized the agencies for being unable to adequately break out and analyze computer and telecommunication costs.[47] GAO officials estimate that the actual level of Federal expenditure for information technology is approximately twice that reflected in the OMB figures, or roughly $30 billion in fiscal year 1986.[48] A further consideration is that, as agencies have grown more sophisticated in identifying costs, they have included more items not captured in previous years, particularly in office automation and telecommunications. Thus, according to GSA, the growth rates for information technology expenditures in OMB's figures are deceptively large because the agencies are now including items that they did not include previously.[49]

Figure 2-2.—Information Technology Obligations in Current and Constant Dollars



SOURCE: Office of Management and Budget, General Services Administration, and the Department of Commerce/National Bureau of Standards, *A Five-Year Plan for Meeting the ADP and Telecommunications Needs of the Federal Government*, June 1985.

---

[44] OMB, GSA, and Commerce/NBS, *A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, June 1985.

[45] The OMB and IDC numbers are only roughly comparable due to differences in data sources and definitions. IDC, "Federal Market Spending Analysis, 1983-88," June 1984.

[46] John McNicholas, OMB, personal communication, February 1986. Also see, e.g., Grace Commission, op. cit.; Ellen Law, "Wright: 'Big Bucks' To Be Invested in ADP," *Government Computer News*, Mar. 8, 1985.

[47] U.S. General Accounting Office, *Accounting for Automatic Data Processing Costs Needs Improvement*, FGMSD-78-14, Feb. 7, 1978.

[48] Walter Anderson, GAO, interview with OTA staff, September 1985.

[49] GSA letter to OTA, September 1985.

Table 2-5.—IDC Projections of Information Technology Sales to the Government

Section		Sales (hundreds of thousands of dollars)			
		Actual 1983	Part of total	Projected 1988	Part of total
1	ADP equipment rental and purchase	$ 2,282	17%	$ 4,046	17%
2	ADP services	1,795	13%	3,392	14%
		$ 4,077	30%	$ 7,438	31%
3	Communication equipment rental and purchase	1,861	14%	3,117	13%
4	Telephone utilities	1,800	13%	2,300	10%
5	Telephone communicaton services (maintenance, technical repair FM)	1,150	8%	2,025	8%
6	R&D electrical and communications	3,832	28%	7,707	32%
	R&D space tracking and data acquisition	171	1%	208	1%
		$ 8,814	64%	$15,357	64%
7	Office equipment	127		109	
8	Office services	42		60	
		$ 169	1%	$ 169	1%
9	Electric and electronic instrument purchase	591		754	
	Electric and electronic instrument maintenance	101		123	
		692	5%	877	4%
	Total	$13,752[a]	100%	$23,841[a]	100%

[a] Excludes Facility Management (primarily Department of Energy) of $8.5 billion.

SOURCE: International Data Corp., "Federal Market Spending Analysis, 1983-88."

Medium- and Large-Scale Computers

GSA reported 18,183 computer central processing units (CPUs) in its revised inventory as of the second quarter of fiscal year 1985. The new inventory contains only computer equipment costing more than $50,000, or with a monthly rental exceeding $1,667. Seventy-nine percent of the CPUs are owned by the Federal Government, and the remainder are leased.[50] Figure 2-3 presents the distribution of dollar value of equipment (that is, all components, including not just CPUs but disk drives, peripherals, etc., that fall above the reporting threshold) by agency. Note that roughly 45 percent of the total is in Department of Defense agencies. OMB has estimated that there will be 25,000 mainframe systems in the government by 1990.[51]

Data from OTA's Federal Agency Data Request strongly support the hypothesis of rapid growth of computer use in government. Of the 142 agency components polled by OTA,[52] figures 2-4 and 2-5 show that the number of mainframe CPUs[53] has more than doubled, from 11,300 in 1980 to 26,700 in 1985, and the number of terminals has increased more than fourfold, from 36,400 in 1980 to over 170,000 in 1985. Defense, Treasury, and NASA account for almost the entire gain in number of CPUs. However, a better indicator of the pervasiveness of information technology may be the number of terminals, in which almost every agency showed dramatic increases between 1980 and 1985.

Microcomputers

Tracking mechanisms are just beginning to catch up to the microcomputer's relatively sudden penetration into the Federal Govern-

---

[50] General Services Administration, *Automatic Data Processing Equipment in the U.S. Government: First and Second Quarter 1985 Summary*. GSA's earlier inventory of ADP equipment regardless of cost had a count of 20,011 CPUs at the end of fiscal year 1983. However, because of data reliability problems in the system, and the paperwork burden on agencies of reporting low dollar-value systems, GSA developed the new system and instituted the $50,000 threshold.

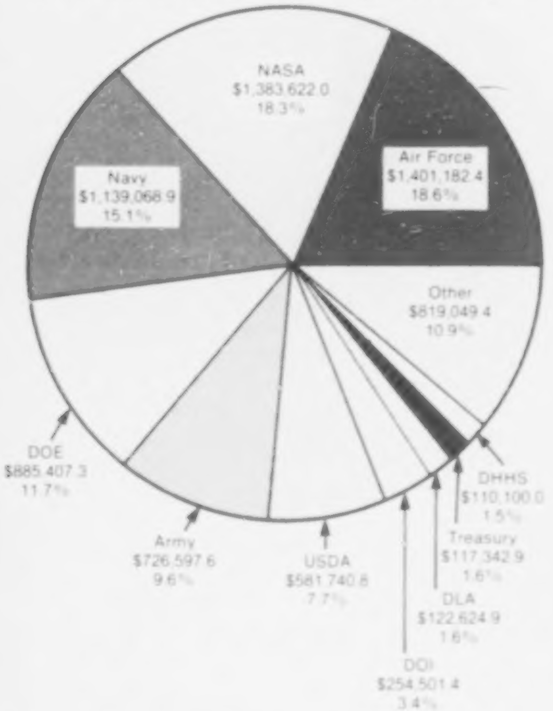
[51] Joseph Wright, Deputy Director, OMB, testimony to Senate Governmental Affairs Subcommittee on Oversight of Government Management, hearings on "Computer Security in the Federal Government and the Private Sector," Oct. 25-26, 1983, p. 52.

[52] OTA's data request was sent to all major units of the cabinet level agencies plus 20 selected independent agencies. Each sub-cabinet agency's response, along with the 20 independent agencies, is counted as a separate response in calculating the total of 142. See app. B for a list of agencies responding.

[53] There were some differences in agencies' interpretation of the wording of OTA's data request. Some agencies included minicomputers in their tally of mainframe CPUs, while others did not.

Figure 2-3.—Distribution of ADPE Dollar Value by Reporting Agency

Total ADPE dollar value (in thousands of dollars): $7,541,237.6



KEY:
NASA - National Aeronautics and Space Administration
DOE - Department of Energy
Army - Department of the Army
USDA - Department of Agriculture
DOI - Department of the Interior
DLA - Defense Logistics Agency
Treasury - Department of the Treasury
DHHS - Department of Health and Human Services

SOURCE: General Services Administration, *Automatic Data Processing Equipment in the U.S. Government,* First and Second Quarter FY 1985 Summary.

ment. Although there is no authoritative count of the number of microcomputers in government, a 1983 GSA report makes a very rough estimate of 82,000 word processors and as many as 210,000 personal computers.[54] GSA has also begun to conduct annual surveys of agency purchases of computers costing less than $10,000. The first survey reported that 7,908 systems costing less than $10,000 were purchased in fiscal year 1983 (excluding NASA); GSA staff considered this number to be low by a factor of three to five times or more. The second survey showed 37,277 units bought in fiscal year 1984, for a total expenditure of $137.2 million[55] (see table 2-6).

In response to OTA's Federal Agency Data Request, agencies reported an increase from 2,307 microcomputers in 1980 to about 100,000 in 1985 (see figure 2-6). Defense was again the largest user with 44 percent of the total reported, but all agencies reported large increases. In many agencies (i.e., Departments of Agriculture, Commerce, Health and Human Services, Interior, Justice, Transportation, Treasury; the Environmental Protection Agency; GSA; NASA; and the Veterans Administration), literally thousands of new machines are being installed compared to almost none 5 years ago—a phenomenal rate of change for the Federal Government that has important implications for management.

In particular, the microcomputer explosion means that agencies must cope with decentralization of information manipulation capabil-

Table 2-6.—Purchase of Small Computers by Federal Agencies, Fiscal Year 1984

Agency	Quantity	Price (thousands)
Department of the Navy	10,649	$28,700
NASA	4,029	14,080
Department of the Air Force	4,009	13,797
Environmental Protection Agency	1,910	9,893
Department of Transportation	1,729	10,324
Department of Agriculture	1,501	5,914
Department of the Interior	1,348	5,364
General Services Administration	1,066	3,988
Department of Energy	924	3,662
Department of Commerce	924	3,698
Subtotal	28,089	$99,420
All others (51 agencies)	9,188	37,800
Total	37,277	$137,220

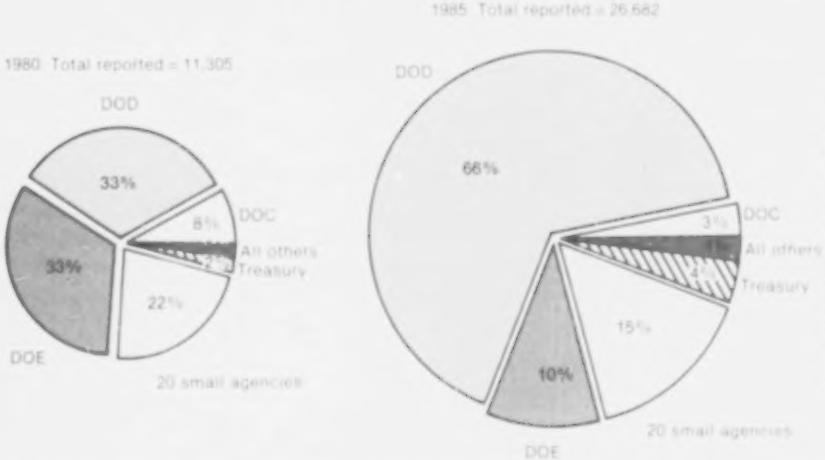
SOURCE: General Services Administration.

---

[54] U.S. General Services Administration, Office of Information Resources Management, *Managing End User Computing in the Federal Government,* June 1983. Ironically, GSA, the official collector of data on government information technology, calculated the 210,000 figure by multiplying a *Time* estimate of 3.5 million personal computers in the country by the government's traditional 6 percent share of the country's computing resources. The 210,000 estimate is probably high because the government owns a disproportionate share of large-scale computing equipment.

[55] GSA reports: "U.S. General Services Administration Survey of Fiscal 1983 Purchases of Small Computers by Federal Agencies," January 1984; "Survey of Small Computers Bought by Government in Fiscal 1984," January 1985.

Figure 2-4.—Mainframe Computers in Federal Agencies



Reported numbers of mainframe computers in Federal agencies

Agency	1980	1985
USDA	13	23
DOC	967	915
DoD	3,765	17,565
Education	1	6
DOE	3,718	2,781
DHHS	48	106
HUD	1	7
DOI	81	250
Justice	26	75
DOL	11	15
State	5	6
DOT	16	15
Treasury	205	1,030
20 small agencies	2,443	3,888
Total	11,305	26,682

NOTE: Consistency in definitions of "mainframe" central processing units cannot be assured because of different interpretations of the term.

SOURCE: OTA Federal Agency Data Request.

ities. In many cases, both in government and industry, information system managers are finding that they must reorient themselves to respond to disparate needs and to encourage, rather than require, microcomputer users to use their equipment productively and to adhere to guidelines for equipment use. For example, many agencies and corporations have developed "information centers" where microcomputer users can receive training, peruse software libraries, and in some cases get access to mainframe data.[56]

Many Federal agencies have begun to focus on the use of microcomputers and on developing supporting efforts. GSA, for example, has published guides for purchasing and managing small computers, has negotiated schedule contracts for agencies to purchase the machines, and has taken the unprecedented step of awarding a contract for the operation of retail computer stores for government agencies at its offices in Washington, DC, Atlanta, and Philadelphia.[57] NBS has issued a variety of guidance documents as well, and has developed a popular microcomputer bulletin board for Federal microcomputer users and managers to share their experiences. The board now includes information not only on microcomputers, but also on computer security and information resources management generally (the latter in cooperation with GSA).[58]

Age and Obsolescence of Federal Computers

One indicator of the health of the Federal Government's procurement process is the extent to which the government is, in fact, using up-to-date technology. There is a long-standing and widespread perception that many of the government's computers are antiquated,

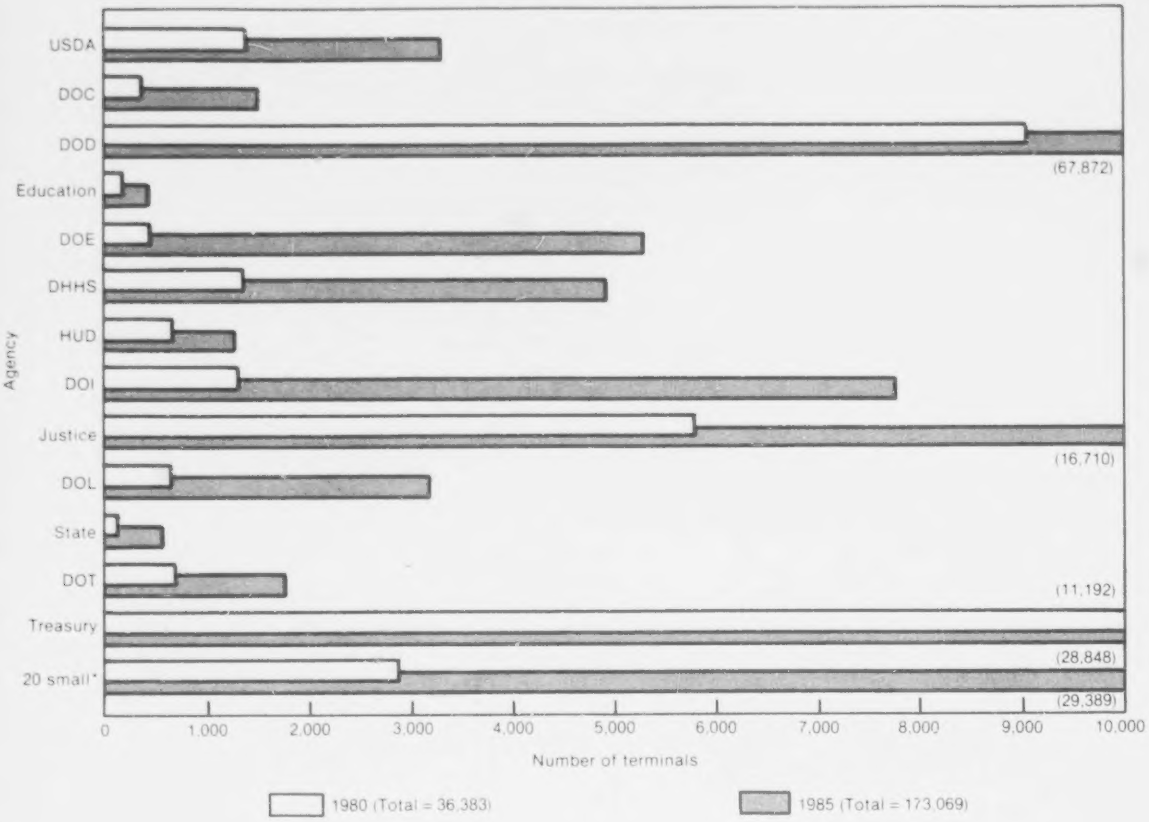
---

[56] Institute of Computer Science and Technology, National Bureau of Standards, *Microcomputers: A Review of Federal Agency Experiences*, NBS Special Publication 500-102, June 1983. See also OTA's study, *Automation of America's Offices*, December 1985, for more extensive discussion of the use of microcomputers in office automation.

[57] See GSA, "Managing End User Computing in the Federal Government," June 1983; "End User's Guide to Buying Small Computers," August 1984. GSA is currently coordinating an interagency study committee that aims to develop further guidance on Federal end-user computing.

[58] NBS, op. cit.; also NBS Special Publication 500-110, *Microcomputers: Introduction to Features and Uses*, March 1984; NBS Special Publication 500-120, *Security of Personal Computer Systems: A Management Guide*, January 1985. NBS staff report that there are roughly 1,100 calls to the bulletin board each month.

Figure 2-5.—Computer Terminals in Federal Agencies



*20 selected independent agencies that received OTA's data request

SOURCE: OTA Federal Agency Data Request

and that the procurement process makes obtaining more effective technology difficult, if not impossible. For example, a 1980 GAO report noted:

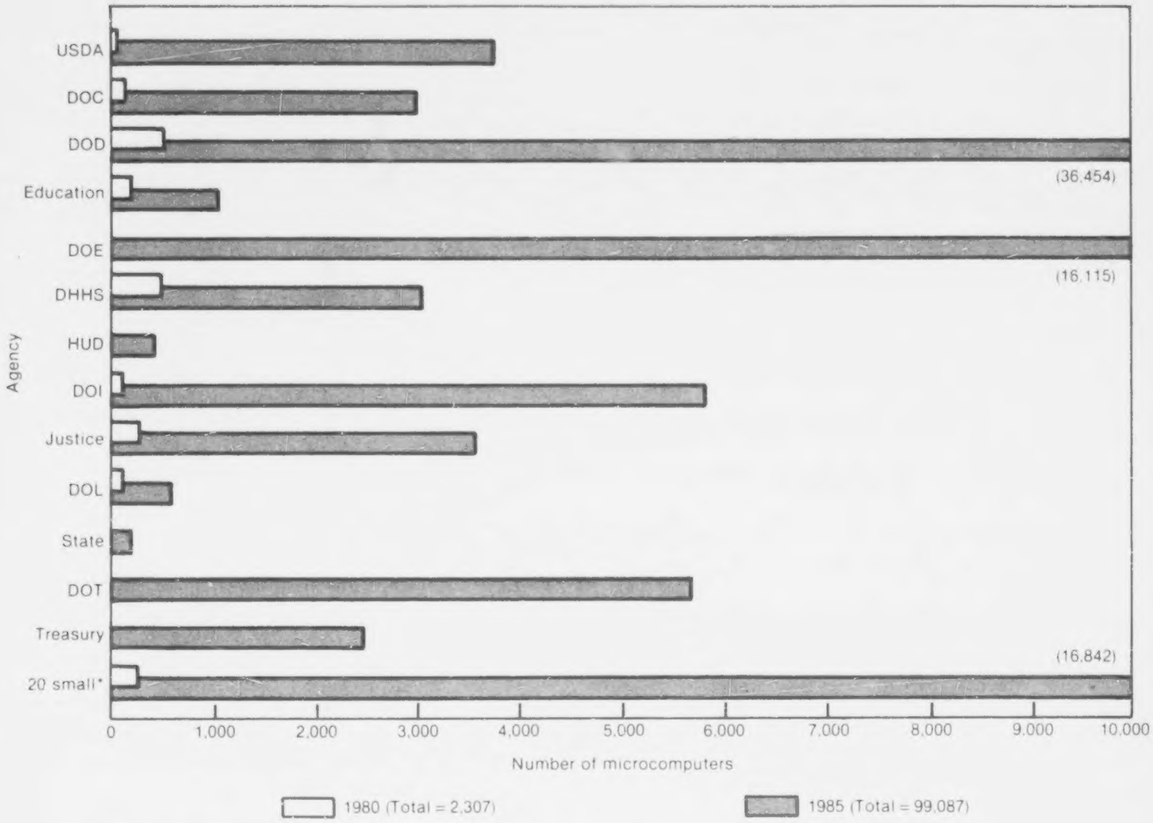
> The current murky acquisition cycle, which is long, complicated, and frustrating, has contributed to the obsolescence of Federal computers.[59]

There are two important caveats in any discussion of the age of Federal information technology. One is that there is tremendous variation among and within agencies. Certain applications, particularly some of those in research and in defense "C^3I" (Command, Control, Communications and Intelligence—as opposed to the routine business of Pentagon budget and logistics, for example), use state-of-the-art information technology tools. Second, there are important differences between the Federal Government and the private sector, such as the complexity of Federal applications, the emphasis in government on maximizing competition and obtaining careful cost justification, and the tax treatment that encourages private companies to purchase new equipment. In addition, Federal expenditures

---

[59] GAO, *Continued Use of Costly, Outmoded Computers in Federal Agencies Can Be Avoided* (Dec. 15, 1980), p. i. See also GAO, *Non-Federal Computer Acquisition Practices Provide Useful Information for Streamlining Federal Methods* (Oct. 2, 1981), for essential background in this area. For a discussion of the popular perception that Federal computers are obsolete and that procurement processes are excessively complex, see A. Neely, "Can Old Computers Learn New Tricks? Federal Managers Try Hi-Tech Comeback," *National Journal*, June 23, 1984; and L. Wynter, "Federal Bid to Update Agencies' Computers Faces Many Obstacles," *Wall Street Journal*, Feb. 13, 1985.

Figure 2-6.—Microcomputers in Federal Agencies



*20 independent agencies selected by OTA to receive the data request

NOTE: The data request used GSA's definition of microcomputer, slightly adapted: "Any microprocessor-based workstation capable of independent use — including stand-alone and networked personal computers, professional computers, intelligent terminals, word processors, and other similar devices — costing less than $10,000 per unit, but excluding peripherals and separately purchased software."

SOURCE: OTA Federal Agency Data Request

and mistakes are much more highly visible than those of the private sector.[60]

Three key reports form the essential background for examining obsolescence in Federal computers. The first was GAO's 1980 report previously mentioned. Focusing on computers that had a central processing unit purchase price of more than $250,000 or a leasing price of over $10,000 per month, GAO concluded (see figure 2-7):[61]

> The Federal inventory of medium- and large-scale computers is outmoded. Of the 1,366 such processors included in the April 1979 inventory, over half were technologically of the 1971 era or earlier. Almost a third of them were technologically 15 years old or older. Only 2 percent used the technology of 1975 or later. Unless action is taken to modernize the government's computers, avoidable costs and unnecessary problems will continue.

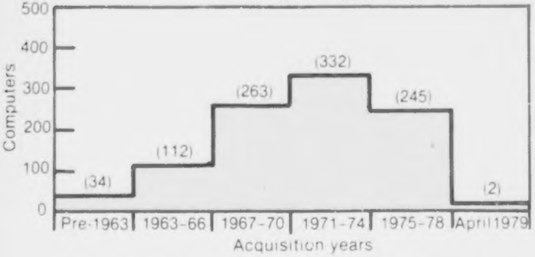
---

[60] See, for example, Mitch Betts, "Speaker Says Bias Colors Criticism of Federal DP Shops," *Computerworld*, May 13, 1985, p. 34. The speaker was Robert Head, a Federal computer veteran and at the time an official of the Federal Computer Performance Evaluation and Simulation Center (FEDSIM).

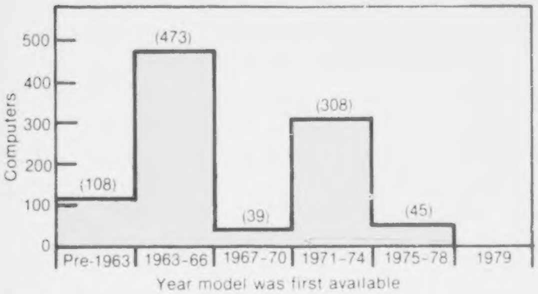
[61] GAO, 1980, op. cit., p. 5.

Figure 2-7.—Age of 978 Large- and Medium-Scale Federal Computers

Based on year acquired



Based on the years these models were first available



SOURCE: U.S. General Accounting Office, *Continued Use of Costly, Outmoded Computers in Federal Agencies Can Be Avoided*, ARMD-81-9, Dec. 15, 1980.

> Our work showed that the operational costs of obsolescent, government-owned equipment can exceed the costs of using newer equipment even if the newer equipment is obtained on a short term lease basis. The maintenance, power, and cooling costs of outmoded, owned equipment were greater than the leasing, maintenance, power, and cooling costs of newer equipment. This alone can justify immediate replacement.[62]

The second key report on Federal ADP obsolescence, by the National Bureau of Standards in 1982 (using fiscal year 1981 data), had a similar though slightly more optimistic conclusion:

> In general, our current statistics indicate that the situation of obsolescence is not as bad as portrayed in the General Accounting Office report, but there is still a large number of older computers in the Federal inventory. Our analysis suggests that certain agencies, particularly the Navy Department, Department of Justice, Department of Commerce, and the Department of Transportation, should analyze their computer inventories to see if upgrading their state of computer technology is in order.[63]

Finally, the third and most recent major study of obsolescence downplays the problem significantly. GSA identified 100 major systems "considered crucial to the nation," and found that "ADPE obsolescence in the Federal Government is not as extensive as has been claimed." GSA defined an obsolete CPU as one that is more than two production cycles old, and assumed an average production cycle for large-scale computers of 4 years. Hence, since the study used fiscal year 1984 data, any machine that has an "original production date" (i.e., was first manufactured) earlier than 1976 would be considered obsolete. Of the 100 systems studied:

- 11 use commercial time-sharing resources, and, as such, are presumed to be processed by modern ADPE;
- 57 are 1976 or newer, and 39 (over two-thirds) of these are supported by CPUs with a 1978 or newer first production date;
- 19 have CPUs with pre-1976 original production dates, but 14 of these are in some stage of upgrade or replacement; i.e., agency procurement request pending, award granted, but equipment not yet installed, etc.; and
- 13 are mixed; i.e., CPUs supporting these systems have first production dates of both pre-1976 and 1976 or newer. (In general, 1976 or newer technology is predominate in these applications, and four of these systems are being upgraded or replaced.)[64]

---

[62] Partly in response to GAO's 1980 report on obsolescence in Federal computers, GSA has since 1982 been granting authority to agencies to conduct "technology updates." This program allows agencies to replace obsolescent computer systems with compatible newer systems of approximately the same computing power, if there are substantial savings. GSA is now reevaluating this program in light of the Competition in Contracting Act.

[63] Martha Gray, National Bureau of Standards, Institute for Computer Sciences and Technology, *Federal ADP Equipment: A Compilation of Statistics—1981*, November 1982, p. 35.

[64] General Services Administration, *Assessing ADPE Obsolescence in Major Federal Systems*, February 1985, p. 9.

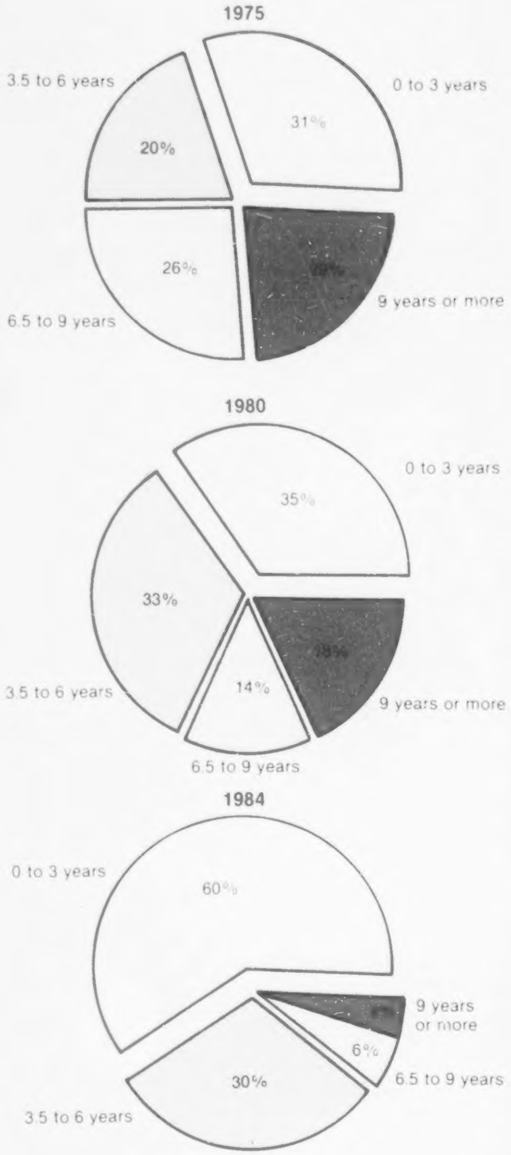
This analysis shows that only 5 percent of these major systems are being totally supported by obsolete CPUs that are not in the process of being upgraded or replaced. In addition, OMB's 1984 5-year plan asserted that "the average length of time in service for Federal computers is decreasing. At the end of fiscal year 1979, it was 7.3 years; at the end of fiscal year 1983, 6.6 years."[65] However, GSA's data, which is the base information for several of these analyses, are known to be inaccurate.[66] GSA's revised database should ultimately provide further information.

Responses to OTA's data request (see figure 2-8) also provided evidence of a modernization trend in Federal computers. When asked to specify the average age of their mainframe computers, the number of agency units reporting average ages of their mainframe computers from 0 to 3 years jumped from 31 percent in 1975 to 60 percent in 1984, and the number of units reporting average ages greater than 6 years declined from 49 percent in 1975 to 11 percent in 1984. Because of methodological differences, OTA's data are not strictly comparable with the length of service data above. For example, OTA's data request asked agencies to report average ages of all of their mainframes. OTA's data may also be optimistic about obsolescence because agency components with only a few newer computers are given the same weight in these statistics as agency components with thousands of computers.

Several other indicators suggest that the obsolescence problem has indeed been improving over the past 5 years:

- Federal agencies have dramatically increased both their overall expenditures for information technology and their capital investment levels. According to OMB

Figure 2-8.—Average Age of Mainframe Computers



NOTE: 134 agency components responded to this question.

SOURCE: OTA Federal Agency Data Request.

---

[65] OMB, GSA, and Commerce/NBS, *A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, April 1984, vol. 1, p. 3.

[66] GSA acknowledged this in its 1985 report, op. cit.

documents, agencies had capital investments for information technology in 1982 of $1.01 billion, 11.2 percent of the $9.1 billion total information technology obligations; obligations soared to $2.86 billion, 19.6 percent of the $14.6 billion total in fiscal year 1985; and eased back down to $2.17 billion, 14.3 percent of the total $15.2 billion in fiscal year 1986.[67]

- In addition to capital investment, agencies also seem to be increasing the proportion of their information technology expenditures that is for commercial services. In 1983 to 1985, the proportion was 44 to 45 percent, but in 1986 the proportion is expected to increase to 50 percent. According to GSA and industry analysts, one can safely assume that commercial vendors of ADP services use relatively up-to-date equipment.[68]
- Similarly, an International Data Corp. forecast expects Federal spending for ADP equipment and supplies (both rental and purchase) to grow from $2.3 billion in 1983 to $4.0 billion in 1988. Particularly high growth is expected in purchases of ADP systems, from $607 million in 1983 to $1.51 billion in 1988.[69] As noted earlier, Gramm-Rudman-Hollings deficit cutting measures are sure to affect planned spending, although the magnitude of these effects is unknown.
- Finally, experts consulted by OTA, both government officials and vendor representatives, generally agree that much modernization has taken place in the last few years, and a great deal more is planned.[70] However, examples of antiquated Federal computers remain.

Length of the Procurement Process

Essentially, as noted earlier in this chapter, the procurement process is in flux. There are few reliable indicators of the health and effectiveness of the process, and the indicators that do exist are mixed.

While the results of OTA's Federal Agency Data Request can only be considered suggestive in this area,[71] they show a fairly consistent pattern. As shown in figure 2-9, the plot of average procurement times peaks at 1 to 1.5 years for both 1980 and 1984, with a substantial number of procurements in the 0.5 to 1 and 2 to 2.5 year slots. Very few procurements were reported to have taken longer than 2.5 years. The most prevalent factors cited for increases in the length of the procurement process were the time it takes to get a delegation of procurement authority from GSA, as well as the changing regulations (especially the Competition in Contracting Act and GSA rules) and the various levels of review and oversight (including preparation of voluminous justification documents) that are required for a large procurement. On the other hand, a few agencies reported that increasing thresholds for delegation of procurement authority from GSA in fact decreased their procurement time.

---

[67] OMB, GSA, and Commerce/NBS, op. cit., April 1983; April 1984; June 1985.

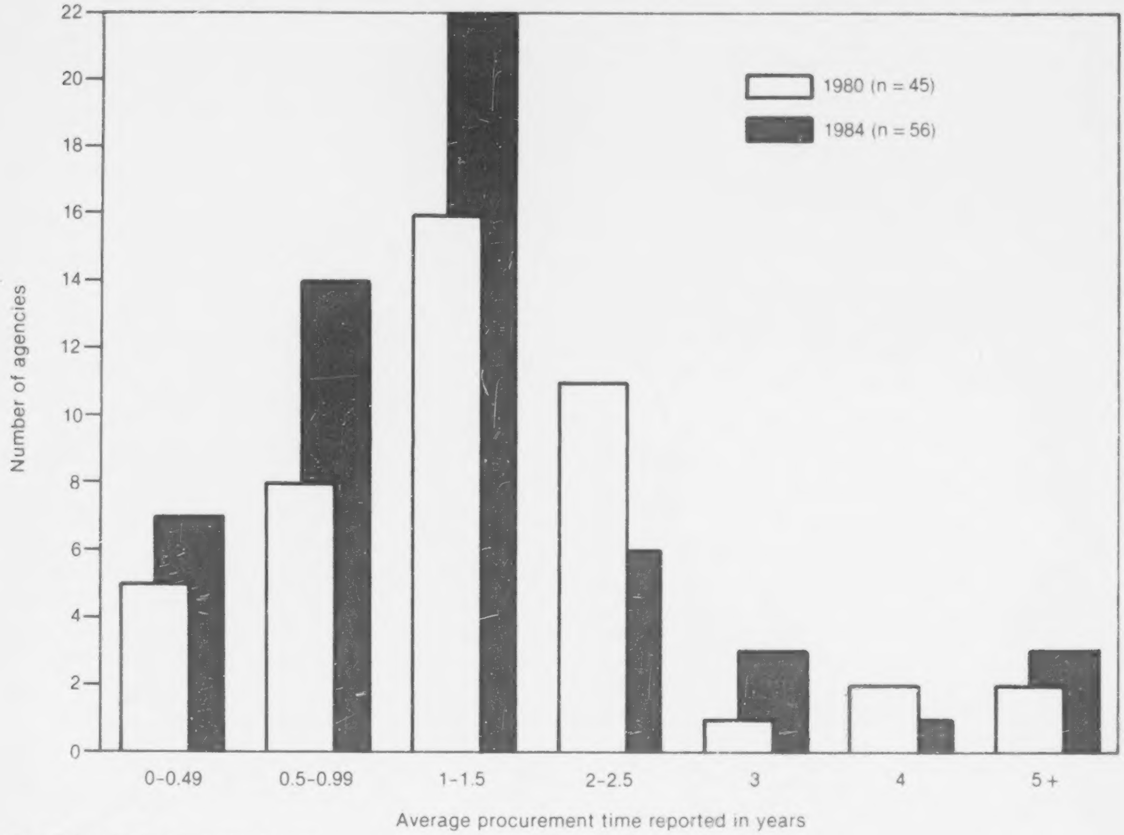
[68] Ibid.; and GSA, *Assessing ADPE Obsolescence*, op. cit.

[69] International Data Corp., "Federal Market Spending Analysis: 1983-1988," June 1984.

[70] This was the sentiment, for example, at OTA's work session on information technology management, procurement, and planning, June 26, 1985. For some of the major planned modernizations, see OMB, GSA, and Commerce/NBS, op. cit., 1985, which describes the system plans for the Patent and Trademark Office Automation Plan, Internal Revenue Service Tax System Redesign, Federal Aviation Administration Advanced Automation Plan, Department of Defense Tri-Service Medical Information System Composite Health Care System, Census Bureau Decennial Census Program, Social Security Administration Systems Modernization Plan, Department of Agriculture Farm Agency System, and Department of Energy Laboratory System.

[71] Of 134 responses total, 80 agency components responded to OTA's request for average procurement times of mainframe computers in 1975, 1980, and 1984. The brevity of the question clearly had some flaws; for example, an average procurement time may not give a good indication of exceptionally long or short procurements; the point at which procurement time begins or ends was not specified; and the data request did not examine software procurement, which clearly deserves study.

Figure 2-9.—Average Procurement Time for Mainframe Computers



SOURCE: OTA Federal Agency Data Request

APPENDIX 2A.—EXCERPTS FROM MAJOR STUDIES AND POLICY ACTIONS IN INFORMATION TECHNOLOGY MANAGEMENT

> The widespread use of electronic systems for handling large volumes of data has developed only in the last few years. . . .We have noted that the general trend has been to use electronic computers in segments of agency operations rather than in systems in which management procedures and controls over related functional areas are fully integrated. . . .The principal recommendation in our report is concerned with the need to establish an effective and coordinated program of joint effort by the interested agencies of the government.
>
> *—Joseph Campbell, Comptroller General, GAO, letter report to Rep. Sam Rayburn, June 27, 1958*

> The findings on the impact of ADP previously reported herein indicate that dynamic leadership of the ADP program of the Federal Government is a vital necessity. Passive, partial, or informal types of leadership have had their place, but have now outworn their usefulness.
>
> *—"Report of Findings and Recommendations Resulting From the Automatic Data Processing (ADP) Responsibilities Study, September 1958-June 1959," Bureau of the Budget, p. 20*

After 6 years, the type of leadership the Bureau of the Budget (BOB) recommended in this early automatic data processing (ADP) management study has yet to be realized. This legislation would establish the authority and provide the operational machinery needed for the effective and efficient management of this costly equipment.

—Senate Report (Government Operations Committee) No. 938, Oct. 22, 1965, To accompany H.R. 4845 ("The Brooks Act"), p. 1

In the case of paperwork, the compartmentalization of policy and operating authorities and functions has resulted in the failure to consider systematically less paperwork-intensive alternatives, the costs involved to everyone when new programs are designed and implemented are not fully taken into account, and citizens are extremely dissatisfied with the manner in which they are served by and interact with their Government.

Therefore the commission concludes that central policy and operating functions and authorities for Government's automatic data processing, statistical, public-use reporting, interagency reporting, forms, microform, word processing, telecommunications and related paperwork, information and communications programs should be brought together in a central management authority. Correspondingly, at the agency level, operating functions and authorities should be consolidated under the direction and control of an appropriate central management authority in each executive department and agency.

—Information Resources Management, Report of the Commission on Federal Paperwork (Washington, DC: GPO, 1977), p. 65

1) The Federal Government needs to take actions that will establish the importance of information technology, provide tools for its management, and set national and federal goals for its productive use.

2) The Federal Government needs to improve and expand its use of modern information technology to increase and enhance the level and quality of governmental service delivery while reducing costs.

3) The Office of Management and Budget needs to establish a policy requiring that costs of data processing be charged back to the using agency and program in program-related terms.

4) The Federal Government needs to set as an objective the removal from service of all information technology components which have outlived their cost-effective life.

5) The Federal Government needs to significantly alter its process for acquiring information technology resources. Increased emphasis should be placed upon the planning, needs definition, and justification phases of acquisition.

6) The Federal Government needs to upgrade the training and career development required for functional managers, reclassify personnel skilled in the management or use of information technology, and establish appropriate career paths for such persons.

7) The program and mission agencies need to be strengthened to meet the general requirements for managerial and technical expertise in information technology. The agencies must have prompt access to resources which can help them solve their problems.

8) The Federal Government needs to institute a research and development program in information technology to meet the needs of the nondefense sector.

9) The Federal Government needs to revitalize its efforts to establish and maintain a standards program for information technology in order to support the economic purchase of equipment and the economic and effective operation of computer resources.

—Information Technology and Governmental Reorganization: Summary of the Federal Data Processing Reorganization Project, OMB, April 1979, pp. 6-18

The Paperwork Reduction Act creates a single control point for the management of Federal information resources. It ends the fragmented responsibility for controlling Federal paperwork burdens which exists today and establishes visible and accountable officials for information management within the Office of Management and Budget and each agency.

—Senate Report (Governmental Affairs Committee) No. 96-930, to accompany the Paperwork Reduction Act of 1980, Sept. 8, 1980, p. 5

The ADP Task Force found that the Federal Government is not effectively managing its information technology resources and, therefore, missing out on substantial potential cost savings. The Government has failed to develop a coherent system for ADP planning and management. As a result, it has not capitalized on the substantial opportunities for cost savings and effectiveness improvement.

—President's Private Sector Survey on Cost Control ("The Grace Commission"), Report on Automated Data Processing/Office Automation, spring-fall 1983, p. iii

Despite substantial improvements, Federal agencies have not realized the efficiency improvements and economic returns that information technology has made possible . . . the little planning that has taken place has not been as concerned with savings and efficiency improvements as it should have been.

To recapture the Government's position as a leader in the efficient and productive use of information technology, the Administration has adopted a three-point strategy: (1) develop and issue effective and up-to-date Government-wide policies, procedures and guidelines; (2) ensure implementation of those policies through earlier policy-level, OMB involvement in the planning and decision-making processes of selected agencies with significant investments in information technology; and (3) develop results-oriented measures of performance to ensure maximum return on the Government's investment in information technology. . . .

- Agencies will be required to document at least a 10 percent return on their information technology investments;
- Agencies will be required to implement standards that foster open systems of communication and permit the exchange of information among systems;
- Greater reliance will be placed on the acquisition of commercially available software to reduce the Government's dependence upon locally developed, customized software.

—Office of Management and Budget, Management of the United States Government Fiscal Year 1986

Chapter 3

Policy Issues in Management, Planning, and Innovation

Contents

Page

Summary 43

Introduction 44

Major Findings 47
  Finding 1 47
  Finding 2 50
  Finding 3 51
  Finding 4 52

Tables

Table No. *Page*

3-1. Dimensions Along Which Agency Planning Styles Differ 46
3-2. Opportunities for Use of Information Technology at Five Key Agencies 49
3-3. Agencies Reporting Current or Planned Use of Certain Information Technology Tools 49

Chapter 3

Policy Issues in Management, Planning, and Innovation

SUMMARY

This chapter examines a set of issues related to information technology management and innovation in Federal agencies. Specific topics that are of interest include the strengths and weaknesses of current agency and governmentwide planning efforts; the adequacy of policies for planning, procurement, and management; the extent to which agencies are using information technology in strategic and innovative ways; the extent to which planning efforts consider the civil liberties impacts of information technology use; and the adequacy of information available to Congress in the areas of planning and management. In this analysis, it is important to note that planning for information technology cannot be divorced from agency planning as a whole, and in fact there should be substantial interaction between the two processes.

Almost since the first uses of computers in the government, there has been a building consensus that the Federal Government's planning in this area is often weak, resulting in serious problems implementing the government's large-scale systems, and in failures to capitalize on opportunities to use information technology. The reasons for this chronic weakness in Federal information technology planning include rapid change in technology, frequent top-level management turnover, changes in political goals, bureaucratic defensiveness, scarce personnel and time, and short-range budget and procurement processes.

OTA's major findings in this area are:

- Effective planning is an essential component of effective use of information technology. Many Federal agencies have begun to develop thoughtful plans. However, many of these efforts appear to have major flaws, including a focus on operational as opposed to strategic plans, a failure to identify innovative opportunities for use of information technology, and a failure to connect planning effectively to implementation.
- The annual "5-year plans" currently published by the Office of Management and Budget (OMB) lack an analysis of agency or governmentwide strategies for using information technology to further government missions. They also do not discuss the security, privacy, and civil liberties implications of information system plans. Without such information, congressional oversight of information technology management and security/privacy issues is much more difficult.
- There are serious deficiencies in the information available to Congress, and to the agencies themselves, on the scope and nature of information technology in use in government. These deficiencies could present difficulties for effective congressional oversight and agency decisionmaking regarding information technology use.

For the Federal Government to improve its effectiveness in using information technology, the quality of information *about* information technology needs to be improved, innovation needs to be encouraged and pursued more vigorously, and strategic planning needs to be significantly strengthened. Though much of this can be done by the executive branch acting alone, Congress can facilitate and encourage some of these actions. OTA's analysis indicates that the following actions warrant congressional as well as executive branch consideration:

- Holding hearings or conducting studies on the accuracy and usefulness of information being collected by the General Services Administration (GSA) and OMB; the extent of innovative uses of information technology in Federal agencies; comparisons between government and private sector information technology planning strategies; the extent to which agencies are using information technology to further government goals; and the effectiveness of the procurement process.

- Encouraging effective use of information technology by giving stronger mandates to central agencies to collect and distribute documentation of innovative applications; designating a formal resource center for information technology planning and innovation; strengthening the role of the National Bureau of Standards (NBS) in providing technology trend information to agencies; enhancing training for information technology planners, procurement officers, and managers; experimentally exempting certain agencies from procurement regulations; and assembling an interdisciplinary team to assist agencies in developing and salvaging major information technology projects.
- Amending the Paperwork Reduction Act to give agencies a clear mandate for strategic planning; to clarify the mandate for the "5-year plan" from the Office of Management and Budget to include information useful to Congress; to specify that agency and governmentwide planning efforts must consider security, privacy, and civil liberties impacts; to strengthen the definition of information resources management (IRM) in the act; and to designate an additional assistant secretary, for some agencies, who would be responsible for IRM.

INTRODUCTION

This chapter examines a set of issues related to information technology management and innovation in Federal agencies. Specific topics that are of interest include the strengths and weaknesses of current agency and governmentwide planning efforts; the adequacy of policies for planning, procurement, and management; the extent to which agencies are using information technology in strategic and innovative ways; the extent to which planning efforts consider the civil liberties impacts of information technology use; and the adequacy of planning and management information available to Congress. In this analysis, it is important to note that planning for information technology cannot be divorced from agency planning as a whole; in fact, there must be substantial interaction between the two processes.

Although different theorists and organizations use different terms, planning efforts generally differ along two dimensions:

1. The length of time considered by the planning process. Generally, plans for more than 1 to 2 years hence are generally considered long term, while others are considered short term.
2. The extent to which plans seek to define new goals and programs. Those that do so are generally termed strategic plans, whereas plans that extrapolate from the current situation and describe the implementation of existing goals and programs are called tactical or operational plans.

There are many permutations of these terms for different planning applications. For example, OMB's guidance for planning strategies defines the different types of planning as follows:[1]

- *Long-term or strategic planning* is a process for defining agency missions and identifying agency goals and objectives as projected over a specified period of time. In the context of automatic data processing (ADP) and telecommunications, long-range planning develops and documents the agency's direction and specifies the activities and resource requirements necessary to support stated missions and objectives.

---

[1] Office of Management and Budget, General Services Administration, and Department of Commerce/National Bureau of Standards, *A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, "Volume 1: Planning Strategies," April 1984, p. 12.

- *Tactical planning* involves identifying and scheduling the appropriate means for attaining the stated objectives of individual ADP and telecommunication activities that support the strategic plan.
- *Operational planning* integrates individual tactical plans and drives the day-to-day activities of line operations.

Private sector planning experts generally place considerably more emphasis on the strategic, goal-seeking aspect of planning. For example, one business administration text defines strategic planning as:

> . . . the continuous process of making present entrepreneurial *(risk-taking) decisions* systematically and with the greatest knowledge of their futurity; organizing systematically the *efforts* needed to carry out these decisions; and measuring the results of these decisions against the expectations through organized, *systematic feedback*.[2]

While there are few, if any, disagreements on the importance of planning to effective use of information technology, on a practical level there are differing notions of what constitutes an effective and realistic plan. Federal information technology managers contacted by OTA often cited the following factors as affecting what is realistically possible from their planning efforts, and what level of effort planning deserves:[3]

- Since information technology is changing so rapidly, it is difficult to anticipate what technology will be available for agency use more than a few years from now.
- The frequent top-level management turnover in the executive branch means frequent shifting of priorities, and thus planning beyond 1 or 2 years often results in (seemingly) wasted effort.
- Agencies' long-range goals, both general and specific to information technology, are determined by a political process that includes, in particular, the White House and Congress. These goals also seem to be frequently shifting.
- Goals that are set forth visibly in long-range plans often become targets for attack by central management agencies or Congress. Thus, it often seems easier to develop information technology capabilities incrementally.
- When personnel and time are scarce, and when the ability of information systems to meet demands reaches a state of crisis, planning seems to be a diversion from survival. This was the case, for example, in the Social Security Administration in the late 1970s; although many believe that it was only by developing a coherent plan for the early 1980s that SSA came out of its tailspin.
- It is difficult to develop goal-oriented, long-range plans when the budget and procurement processes are relatively rigid and short range. This factor has intensified after enactment of the Gramm-Rudman-Hollings deficit reduction act, since uncertainty about future budgets has been increased considerably.

The combination of these factors tends to push agencies toward incremental, operational plans, as opposed to strategic plans. Nevertheless, there has been progress in the quality and foresight of government information technology planning. As noted in chapter 2, both GSA and OMB have given high visibility to the need for planning and have issued a variety of guidance documents to assist agencies in the process. GSA, for example, defines a generic planning process to include seven steps:[4]

---

[2] Peter Drucker, *Management* (New York: Harper & Row, 1974), p. 125 (emphasis original).

[3] While these perceptions are not necessarily correct or desirable indicators of the current situation, it is OTA's assessment that they are reasonably widely held in the Federal information technology management community. There are, of course, some exceptions, and as will be discussed below, many agencies have proceeded in developing long-range plans despite these factors.

[4] General Services Administration, *IRM Review Handbook*, 1985, p. 39.

1. update agencywide inventories of information resources;
2. define the missions, broad objectives, and policies of the IRM organization;
3. develop approaches for achieving agency missions and broad IRM objectives within the context of existing policies;
4. prepare specific top-down planning directions (call for plans);
5. develop, consolidate, and approve detailed plans and budgets;
6. prepare supplemental analyses; and
7. prepare progress reports based on performance against the plans.

GSA has also recently established a small group to provide planning assistance to agencies on a reimbursable basis.[5]

Clearly, different planning styles are appropriate for agencies differing in mission, structure, and size. Table 3-1 shows some of the dimensions along which agency planning styles differ. Nevertheless, the standards by which most experts would judge a planning process to be effective are reasonably consistent. OTA found that the following criteria are useful in judging planning effectiveness, both at the agency and governmentwide levels:

- **Do information technology plans support overall agency plans?** Clearly, the overriding function of a plan is to help the agency pursue its mission. This requires linking information technology plans to the agency's overall plans. To the extent that overall agency planning efforts are weak, information technology plans may be flawed as well.
- **Does the plan identify opportunities for coordination of information technology projects?** Another role of a plan is to allow coordination of the agency's resources in pursuing various projects, and to ensure that systems developed will be compatible.
- **Does the plan identify opportunities for innovative uses of information technology to pursue agency missions?** This is the strategic aspect of an information technology plan, where a planning effort should catalyze creative thinking by agency staff on ways to deliver services in new ways or to improve efficiency.

Table 3-1.—Dimensions Along Which Agency Planning Styles Differ

Goal driven ..... Incremental
Long term ..... Short term

Some agencies take a long-term, strategic approach to information technology planning looking for ways to integrate information technology into the agency strategic plans. Other agencies look primarily to modest improvements they can make in existing systems that will enable them to do their job better.

Centralized ..... Distributed

Agency planning can vary from highly centralized, headquarters based approaches to highly decentralized, localized planning by individual agencies, regional offices, or field offices.

Top down ..... Bottom up
Hierarchical ..... Participatory

Some agencies encourage participation from line offices and interested individuals. Other agencies prefer to have top managers create the framework within which other managers operate. Most agencies use some mix of the two.

Structured ..... Informal, ad hoc

While the requirements of the Paperwork Reduction Act of 1980 and the resulting OMB and GSA guidance have increased the formalism of all agency plans, styles continue to range from highly structured, rigidly scheduled, formal processes to informal assessments of future information technology needs and potential.

Integrated ..... Fragmented

Several agencies look at their information technology resources in an integrated, system wide manner. Others take a less coherent, more fragmented approach by planning the future of individual technologies, databases, or pieces of hardware.

Security/privacy ..... Efficiency/access

Agencies differ in the degree to which they pay attention to security and privacy issues. Some are concerned primarily with increasing efficiency of operations and providing access to internal and external authorized users. Others take great pains to protect the security of the system and the integrity of data.

Forefront technology ..... Established technology

Some Federal agencies are dependent on leading edge or state-of-the-art technologies such as supercomputers. Others only need established routine technologies such as personal computers or office automation equipment.

SOURCE: J.F. Coates, Inc., *Scenarios of Five Federal Agencies as Shaped By Information Technology*, OTA contractor report, June 1985.

GSA began the Federal IRM Planning Support Program in 1983; in fiscal year 1985 it had 13 planning specialists working on 18 active programs, providing roughly $1 million in reimbursable services to the agencies. OMB's Bulletin 85-12 said that OMB asked GSA to construct a database of current agency information resources and major proposals. In GSA's review comments to OTA, GSA said that this database was in fact stymied because OMB was not supporting its development.

- **Does the plan incorporate concerns for security, privacy, and fair information practices at an early stage in the planning process?** While there is little dispute that the best way to design a secure information system is to consider security throughout the planning, implementation, and use of a system (see ch. 4), this point is often not explicitly recognized by planners. Similarly, concerns for privacy and fair information practices are most easily accommodated when they are introduced at an early stage of system planning.
- **Does the planning process provide a mechanism for interested publics to provide input into major projects for public services or information dissemination?** Obtaining the views of those who will be significantly affected by a major project can help avoid unanticipated pitfalls and make the system more useful. Several examples can be found in major projects for electronic dissemination of information (see ch. 7).
- **Does the process involve both management and operating levels of the organization so that they (on the whole) are committed to implementation of the plan?** The experiences of government and private sector planners indicate that those who are to execute the plan must be part of the planning process, and must largely support the plan. Otherwise, a well-crafted plan can become simply irrelevant to the organization's activities.

MAJOR FINDINGS

Finding 1

Effective planning is an essential component of effective use of information technology. Many Federal agencies have begun to develop thoughtful plans. However, many of these efforts appear to have flaws, including a focus on operational as opposed to strategic plans, a failure to identify innovative opportunities for use of information technology, and a failure to connect planning effectively to implementation.

There is almost no disagreement on the importance of planning for information technology use, both in government and in business. While there may be differences among Federal officials about the feasibility of long-term planning in the Federal Government's bureaucratic environment, it is well understood that planning for information technology is essential to enhance the ability of an agency to use the technology well, especially when complex systems are involved.

The results of OTA's Federal Agency Data Request indicate that despite the problems and criticisms there are substantial planning efforts under way. Many agencies' plans appear to set appropriate goals, and are carefully prepared, detailed, and useful. Despite these efforts, however, many of the plans seem to suffer from a similar set of problems.

Focus on the short-range. Although most agencies have developed 5-year plans as a result of OMB's guidelines and requirements, only a few of the plans devote much effort to years 3 to 5, or develop the plan in a truly "strategic" fashion—that is, seeking out new aspects of their mission and opportunities for information technology to improve the agency.[6] In some cases, this may be because staff assigned to prepare the plan do not have the authority to develop strategic goals, or do not have the attention of the agency's top management. Moreover, in most cases, the later years of a 5-year plan are not considered credible because they involve acquisitions not yet approved by GSA and Congress, and from prior experience most bureaucrats expect that the approval process will alter the future significantly, for good or ill. This factor provides further incentive for agencies to spend less effort on long-range planning. Ironically, the central management agencies would argue that a carefully prepared long-range plan should help budget requests survive the approval process without major upheaval,[7] and that such a plan is the only way to make substantial progress in the agency's use of information technology.

---

[6] An interesting exception seems to be the Department of Agriculture, which has published a small monograph, "The Future of Information Resources Management in the Department of Agriculture (A Strategic Framework)," April 1985. The monograph, used in concert with USDA's 5-year plan, sets forth broader goals and opportunities for use of information technology.

OMB has recognized the scarcity of long-term planning. As its deputy director noted,

> So far, few agencies have taken advantage of the opportunities that have really been offered by modern information technology . . . we have not had enough attention paid to long-term planning for ADP processing and telecommunications.[8]

As a response, OMB devoted the bulk of volume 1 of the 1984 5-year plan to a tutorial on effective planning, and to examples of agencies that do have a significant planning process. Also, in OMB's latest guidance on planning, Bulletin 85-12 (Mar. 29, 1985), OMB tried to adapt these incentives so that good planning would more clearly lead to easier acquisitions. The bulletin, which requests a variety of planning information from agencies, states that acquisitions that are approved as part of planning and management reviews in the spring will have a "shortened and simplified" budget approval process in the fall.[9]

Failure to identify innovative opportunities. In addition to meeting current operational needs, long-term planning is necessary for agencies to take advantage of opportunities to use new information technology tools in effective and innovative ways. OTA found that there are many such opportunities, but that only in a few cases are agencies using innovative tools now, or planning their use. Table 3-2 shows some examples of information technology opportunities for five selected agencies. Thus, for the Social Security Administration, some of the opportunities for change that could be facilitated by information technology include the use of electronic bulletin boards and automated telephone information services in field offices to communicate with clients, expanded use of direct deposit, and possibly the use of "smart cards" (credit-card-sized electronic memories) to record the earnings of each worker. While the specific changes postulated in table 3-2 are speculative, similar opportunities for productive change with concerted attention to information technology were evident in virtually every agency examined by OTA.[10]

One imperfect index of an agency's ability to identify innovative opportunities is the extent to which it is planning uses for information technology beyond the conventional data processing and office automation tasks. OTA asked agencies to indicate whether they had used, were currently using, or were planning to use a variety of new information technology tools ranging from videoconferencing to artificial intelligence. Table 3-3 summarizes the responses. The only techniques currently used by most agencies are electronic mail and audio-conferencing (conference calls), although roughly 30 percent of the agencies said they plan to use teleconferencing (one-way video, two-way audio), optical disk storage, and expert systems.

---

[7] There are at least a few examples where this has occurred. A Department of Justice manager, for instance, reported that because they take the planning process seriously (and use some bureaucratic resourcefulness) they have a considerably easier time with oversight and approval of their plans, and actually follow the plans for the most part. (Frank Guglielmo, Acting Director, Computer Technology and Telecommunications Staff, Office of Information Technology, Department of Justice, "Streamlining Acquisition," address to Government Computer Expo, Washington, DC, June 13, 1985.)

[8] Joseph Wright, testimony to House Science and Technology Subcommittee on Transportation, Aviation, and Materials, hearings on "Computer and Communications Security and Privacy," Sept. 24, 1984, p. 4.

[9] As might be expected, efforts by central management agencies to "collect information" are viewed with some suspicion by line agencies. One cabinet agency told OTA in review comments that it felt the general perception among agency staff was that Bulletin 85-12 was a way for OMB to find places to cut budgets and reduce personnel, not necessarily improve agency strategic planning. The same agency said that it felt OMB's promise for a "shortened and simplified" fall budget approval process was falsified by the fact that, as of October 1985, no one at OMB had indicated they had read their plan submitted in April 1985.

[10] See, for example, J.F. Coates, Inc., *Scenarios of Five Federal Agencies As Shaped by Information Technology*, OTA contractor report, June 21, 1985. This report examined and developed scenarios for the National Oceanic and Atmospheric Administration, Bureau of the Census, Internal Revenue Service, Environmental Protection Agency, and Social Security Administration.

Table 3-2.—Opportunities for Use of Information Technology at Five Key Agencies

Agency/possible use of information technology

Social Security Administration:
- Use of electronic bulletin boards and automated telephone inquiry systems to communicate with clients.
- Expanded use of direct electronic deposit of social security payments.
- Use of smart cards (credit-card-sized electronic memories) for each individual to store his/her earnings records.

Internal Revenue Service:
- Electronic submission of tax returns.
- Increased use of optical character readers to scan returns submitted.
- IRS development or certification of software used to prepare tax returns.
- Use of optical disks to store returns.
- Use of expert systems to assist in auditing.
- Use of computer auditing to closely monitor access to taxpayer information in order to protect privacy.

Bureau of the Census:
- Use of portable data terminals and computer-assisted telephone interviewing for census workers to gather and transmit information.
- Use of expert systems to probe data for errors and trends.
- Overall shift from paper to electronic systems and products, allowing census reports in months instead of four years, and facilitating possible shift to rolling census instead of decennial census.
- More and better data available to public on diskettes.

Environmental Protection Agency:
- Integration of databases storing information on air, water, land quality, supported by sophisticated database management systems, allowing more complex and integrated analyses of health risks.
- Use of robots to implant, repair, and retrieve microprocessor-based environmental monitoring devices.
- Use of smart cards for individuals to record their exposure to environmental hazards.
- Use of expert systems to review environmental impact statements, and examine data for errors and trends.
- Public access to computer models used in environmental decisionmaking.

National Oceanic and Atmospheric Administration:
- Use of supercomputers and expert systems to develop 20-day weather forecasting capability.
- Use of microprocessor-based weather data collection stations to decrease costs and improve forecast accuracy.

NOTE: The specific activities and changes outlined above are intended only as suggestive of possible opportunities related to use of information technology, and not as judgments about their desirability or likelihood.

SOURCE: J.F. Coates, Inc., "Scenarios of Five Federal Agencies (1991-1995) as Shaped by Information Technology," OTA contractor report, June 1985.

Table 3-3.—Agencies Reporting Current or Planned Use of Certain Information Technology Tools

	Currently using		Planning to use	
Technology	#	%	#	%
Audio-conferencing	84	62.7	86	64.2
Teleconferencing	23	17.2	42	31.3
Videoconferencing	10	7.5	30	22.4
Computer-conferencing	16	11.9	29	21.6
Teletext	21	15.7	26	19.4
Videotext	9	6.7	14	10.4
Cable television	14	10.4	20	14.9
Interactive cable	3	2.2	15	11.2
Expert systems/AI	14	10.4	43	32.1
Electronic mail	97	72.4	115	85.8
Voice mail	9	6.7	35	26.1
Optical disks	6	4.5	39	29.1

NOTE: 134 components reporting.

SOURCE: OTA Federal Agency Data Request.

Even though a significant minority of agencies are pursuing the use of advanced information technology tools, most agencies do not seem to be pursuing these (or other) kinds of innovations. While it is likely that some agencies are not pursuing information technology innovations because they do not expect them to be useful, many others are either unaware of potential useful applications or feel that innovation is too risky and likely to come under fire by top agency management, OMB, or Congress. There is no formal support mechanism for agencies considering innovative uses of information technology to obtain information or technical expertise, or to share experiences.

Failure to connect planning effectively to implementation. Perhaps the most serious flaw in the planning process, which often cannot be anticipated in advance, occurs at the implementation stage. Some of these problems are the result of circumstances difficult to foresee, even though agencies tried to implement their plan.[11] In other cases, the agency is simply not organized to carry out the plan, the planning staff is isolated from the operational staff, or staff pay little attention to the plan.[12]

---

[11] For example, a top GAO official said that even though the Federal Aviation Administration (FAA) had done a careful planning job, their huge system upgrade was having serious unforeseen problems in the "benchmarking" process, where the ability of different systems to meet FAA's needs was being tested. (Warren Reed, GAO, "Coping With Policies and Procedures," address to Government Computer Expo, Washington, DC, June 12, 1985).

[12] J.F. Coates, Inc., "Planning for Federal Information Technology: Continuity and Conflict," ch. 7 in J.F. Coates, Inc., op. cit., May 24, 1985, based on interviews with agency officials and literature analysis.

Finding 2

The annual 5-year plans currently published by the Office of Management and Budget lack an analysis of agency or governmentwide strategies for using information technology to further government missions. They also do not discuss the security, privacy, and civil liberties implications of information system plans. Without such information, congressional oversight of information technology management and security/privacy issues is much more difficult.

While the Paperwork Reduction Act of 1980 required OMB to develop a "5-year plan for meeting the automatic data processing and telecommunications needs of the Federal Government," (Section 3505, paragraph 3(E)), the resulting documents do not constitute such a plan, although they do provide some useful information.[13] The 1985 report, for example, contains:

- summary data on Federal expenditures for information technology;
- brief advice to agencies on planning;
- a brief description (one to two pages each) of eight of the largest Federal information systems and their relation to agency mission;
- some information on technical trends in computers and telecommunications, developed with the assistance of NBS; and
- an appendix volume that simply lists the major tentative acquisition plans of Federal agencies, primarily for interested vendors.

OMB acknowledges that the 5-year plans are not really plans. The 1984 plan, for example, notes that the 1983 plan:

> . . . was less a comprehensive plan than a compilation of planning information designed: 1) to assist agencies in preparing their plans; and 2) to inform equipment and services vendors about potential Federal marketing opportunities.[14]

Further, the 1985 report argues that a governmentwide planning document would be unworkable:

> Governmentwide planning is made difficult by the size and diversity of the Federal Government. This leads us to focus on planning efforts at the agency level, since agency goals can be specified more clearly than can goals for the government as a whole. The task of governmentwide planning then becomes one of: (1) specifying the rules for agency planners who develop plans to achieve agency goals, (2) reviewing their success in complying with those rules, and (3) intervening in cases where individual agency planning efforts would produce sub-optimal results.[15]

Despite OMB's skepticism about governmentwide planning, there are "macro-level" goals for the government that are useful and productive to establish—an example is OMB's goal to refocus more attention on software and software maintenance, and to reduce software maintenance expenses by 25 percent and full-time equivalent employees by 5,000, by 1988.[16]

Although clearly there are certain aspects of a detailed governmentwide plan that could become unwieldy, there are several kinds of information not included in these reports that could be useful for congressional oversight needs. In particular, the reports do not shed much light on the different strategies used by agencies to meet their ADP and telecommunication needs, or on the ways in which the agencies are using information technology to further their missions. Information of this kind could help congressional committees compare the strategies of various agencies, assess how information technology shapes new opportunities in Federal agencies' missions, oversee the effectiveness of the Brooks Act and the Paperwork Reduction Act, and possibly develop useful measures to amend these acts. It could also help agencies communicate with one another and pursue joint ventures.

---

[13] *A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government*, April 1983 (1st ed.), April 1984 (2d ed.), and June 1985 (3d ed.). While the publication of the plans is coordinated by OMB, they are a joint effort between OMB, GSA, and the NBS Institute for Computer Sciences and Technology.

[14] *A Five-Year Plan*, 1984, op. cit., p. v. OMB's staff also acknowledged this point at OTA's work session on information technology management, planning, and procurement, June 26, 1985.

[15] *A Five-Year Plan*, 1985, op. cit., p. 17.

[16] OMB, *Management of the United States Government Fiscal Year 1986*.

Gradually, the 5-year plans have become more comprehensive. The 1985 plan, for example, does include descriptions of eight major information systems and their connection to the agency mission. However, the description is too short to provide much insight, and no analysis of agency strategy is included. Further, OMB included in the 1985 plan a list of the titles of major Federal information systems, which were gleaned from agencies' submissions in response to Bulletin 85-12 (see previous finding). Although merely providing the titles of information systems is not very helpful for oversight purposes, the responses to Bulletin 85-12 may be a promising source of information for more substantive analysis of agency strategies in future 5-year plans.

There is one area of congressional interest that neither the OMB plan nor the agency plans are designed to address—the implications of information technology use for privacy and civil liberties, as discussed in OTA's reports on *Electronic Record Systems and Individual Privacy* (forthcoming) and *Electronic Surveillance and Civil Liberties* (October 1985). Congress could ask for an analysis of agency strategies for use of ADP and telecommunications that includes identifying major potential implications for privacy and civil liberties, and describing agency plans for responding to these implications.

Finding 3

There are serious deficiencies in the information available to Congress, and to the agencies themselves, about the scope and nature of information technology in use in the Federal Government. These restrictions could present difficulties for effective congressional oversight and agency decisionmaking regarding information technology use.

OTA found that two kinds of information, currently unavailable, would be useful to Congress in oversight of both information technology policies generally, and of the management of specific agencies:

1. Broad overview data about trends in information technology use in the Federal Government. These would include, for example, both a governmentwide analysis and an agency-by-agency breakdown of:
   - the number of mainframes, minicomputers, and microcomputers in use;
   - investment in software, both custom and off-the-shelf;
   - investment in telecommunications;
   - number and cost of information technology personnel by function (e.g., operations, management, planning, budgeting); and
   - historical and projected trends in these data.

This information would enable Congress to gain an overall sense of the pervasiveness of information technology in government as a whole and in the various agencies; to judge the urgency of congressional attention in computer-related policy areas, such as computer crime; and to assess the rate of change in use and cost of technology in government. With this information, both Congress and executive agencies could evaluate possible changing missions and opportunities for new services and efficiency increases.

2. An evaluation of the extent to which each agency is exploiting innovative information technology tools to accomplish its missions. Gathering this data could take the form of a survey similar to OTA's Federal Agency Data Request, which asked agencies to indicate whether they were using a particular technique and to describe that use briefly. This information could provide Congress with an "early warning" about coming trends in technology use and the ability to assess the level of innovation in different agencies. Such information could also be disseminated to allow other agencies to identify similar opportunities to further their missions.

This description of information useful to Congress is only a starting point, and clearly

Congress itself should determine its information needs. However, using the above as a basis, it is clear that existing information sources only begin to meet these needs.

The apparatus for collecting information about Federal use of information technology is in flux. Several mechanisms have been discontinued or restricted. In particular, after fiscal year 1983, GSA stopped systematically collecting information regarding the number and cost of computers costing less than $50,000. On the other hand, GSA's revised inventory system is intended to be more accurate than the previous one, and on the basis of their first reports, the new system is promising as a source of data on trends in mainframes and more expensive peripherals. (See discussion in Finding 1.[17]) Further, OMB's 5-year plans and OMB's Bulletin 85-12 are improving as sources of information, as noted above.

However, these improvements still leave major gaps in information about software, telecommunications, personnel, and use of emerging technologies. For example, as noted in the previous finding, GSA's annual surveys on microcomputer purchase in the government provide some information, but do not indicate the total number of machines in use. GSA has also discontinued its management information system for keeping track of communications use and expenses.[18]

Perhaps a more troubling issue is that agencies themselves may not have complete information about the technology they use to fulfill their missions. Each agency is mandated by the Paperwork Reduction Act to "systematically inventory" its major information systems (Section 3506, part (c)(1) of Public Law 96-511). Thus, at least in theory, agencies should have reliable data on their information technology use even if centralized data are inadequate. However, there is a clear consensus among government ADP experts that most agencies do not have such systematic and reliable records.[19]

Although OTA acknowledges that gathering data has significant costs and the need for information should be carefully evaluated, overall there appear to be significant gaps in available data that could hamper both effective policymaking and understanding of the information technology transition under way in government, as well as decisionmaking by the agencies themselves. Further, in the absence of reliable information, much effort can be wasted arguing about estimates.[20]

Finding 4

Possible actions to improve information technology management, planning, and innovation include: hearings and studies to improve the accuracy and usefulness of available information, new or strengthened mechanisms for exchanging learning and encouraging innovation, and amendments to the Paperwork Reduction Act.

Since the technology and the administrative environment for Federal information technology are in rapid flux, information technology management is a moving target for congressional policy. Yet, it is widely agreed that government is becoming increasingly dependent on information and information technology. This situation calls for policies and oversight procedures that are flexible and anticipatory to the greatest extent possible, at each level of policymaking for information technology management. More specifically, the goal of being flexible and anticipatory implies that both policymakers and the agencies themselves:

---

[17] The data in the previous system were suspect. For example, a 1985 GAO report noted:

> GSA's data base of the government's inventory of computer equipment has been inaccurate for some time. In attempting to use the data base to select review sites, GAO initially contacted eight computer installations and found errors in the data base for six, which prevented GAO from including them in this review. For example, at two sites, equipment listed on the inventory was not installed, and officials did not know whether it had ever been installed.

General Accounting Office, *Effective Management of Computer Leasing Needed To Reduce Government Costs*, IMTEC-85-3, Mar. 21, 1985, p. iii.

[18] Federal Property Management Regulations, Temporary Regulation F-502, *Federal Register*, Oct. 25, 1983.

[19] Reed, op. cit.

[20] See, for example, Frank Carr, "Government IRM Fact and Fiction," *Government Computer News*, Sept. 17, 1984. The development of reliable data about use of information technology need not involve a complete census of the government in every case. Authoritative statistical estimates may be quite useful for policymaking purposes.

- have reliable information on the use of information technology, and on the trends in that use;
- assess on an ongoing basis the ways in which agencies can use information technology to further their missions; and
- facilitate and reward innovation, as well as expect occasional failure as a cost of attempts to use technology effectively and innovatively.

Though many improvements can be made by the executive branch acting alone, Congress can facilitate and encourage such actions. OTA's analysis indicates that the following actions warrant consideration:

Hearings or studies to improve the information available for oversight and policymaking on information technology management.

OTA found that, as noted in Findings 2 and 3, considerable gaps exist in the information available that hamper policymaking and oversight. Apparently, agencies themselves often do not have good inventories of information technology use, and the governmentwide inventories are limited in scope and reliability. Beyond simply counting and describing the systems in use, there is also no clear mechanism to obtain information about the effects of information technology use on the mission of the agency, and about future plans for information technology use. See the discussion in Finding 3, above, for an elaboration of the kinds of information that could be useful.

Hearings or studies (or related activities, like conferences and workshops) could be conducted on:

- *The accuracy and usefulness of information being collected by GSA and OMB.* Hearings or studies on this topic could also help Congress to define the kinds of information that would be most helpful in its policymaking and oversight.
- *Information technology planning, focusing on planning for innovative applications of information technology in government, and on drawing private sector expertise into the Federal planning process.* Such hearings or studies could serve as forums for agencies and private sector organizations to exchange ideas on uses of information technology and on planning techniques, and could facilitate congressional oversight.
- *Information technology management generally, analyzing the extent to which agencies are using information technology to further government goals.*[21] Most of the oversight hearings on the Paperwork Reduction Act have concentrated on the paperwork reduction aspects, rather than information technology management issues. Congressional hearings could closely examine the new OMB circular on information resources management (see ch. 2). The House Government Operations Subcommittee on Government Information has already held hearings on the information dissemination portion of the circular.
- *The effectiveness of the procurement process for Federal information technology.* In particular, areas where current information is scarce or contradictory include the obsolescence of Federal information technology, the effect of the Competition in Contracting Act on ADP procurements, the extent to which current procurement processes present a barrier to effective and innovative use of information technology, and the staffing and training in procurement offices that handle ADP.

New or strengthened mechanisms to encourage innovation in information technology use.

A set of hearings with a similar goal was held more than a decade ago. See *Federal Information Systems and Plans—Federal Use and Development of Advanced Information Technology*, hearings before a Subcommittee of the House Committee on Government Operations, April, June, and July 1973, and January and February 1974.

OTA found that there is a need for more mechanisms in the government whereby agencies can share information about effective uses of information technology. Clearly, this already happens in a variety of ways—at conferences, multi-agency meetings, and educational programs, through publications distributed by agencies, through NBS documents, and through personal contacts. However, NBS, OMB, and GSA could be given stronger mandates to collect and distribute documentation of innovative applications (the hearings described above could become a forum for sharing such ideas and plans).

Based on much of the evidence cited in the "background" and "findings" sections above, it is clear that many agencies need assistance in developing effective planning processes and identifying opportunities for information technology innovations. OMB, GSA, and the General Accounting Office (GAO) have recognized this need, in part, by providing handbooks and other guidance material on planning. These are promising initiatives, and Congress may wish to oversee the adequacy of these support efforts.

Another option would be to consider designating a formal resource center for information technology innovation and planning, either at GSA or NBS, and/or use personnel detailed from line agencies on a rotating basis. Such a center could provide training for agency staff in planning related to information technology, and could also establish a formal mechanism—such as an interagency committee or regular series of conferences—to allow agencies to coordinate their planning efforts and share expertise.

Another kind of support that agencies need in developing long-range plans is information on technology trends—e.g., the processing speeds and architectures one can expect from computers 3 or 5 years hence. Until recently, the Institute for Computer Sciences and Technology (ICST) at NBS provided such support for agencies.[22] However, because of recent disagreements over the budget at NBS, the agency will no longer contract for any original research in technology trends, but will instead rely on published literature and subscriptions to consulting services. While many of these services provide excellent technology trend data, the Federal Government's information technology use tends to be different from that of the private sector in several ways—including extremely large databases and a more diverse mix of vendors—that may make it useful to have customized trend information.

OMB itself argued for a strong centralized technology trend function in its 1984 5-year plan: "It therefore makes sense for agencies to band together to fund a cooperative forecast, which concentrates on areas of mutual interest."[23] And indeed, it is well within the Brooks Act mandate for NBS to provide such technical resources to the agencies. If Congress agrees that such a resource is appropriate, it may wish to strengthen the function at NBS or designate a similar function in some other agency. In addition, the administration has repeatedly proposed to eliminate or drastically cut back ICST at NBS,[24] and Congress and the executive branch may want to examine the implications of this move for planning support, as well as for information security support and other areas (see ch. 4).

Another set of possibilities for encouraging innovation and effective use of information technology involves the procurement process. Enhanced training for ADP procurement officers, and for managers who are planning and implementing large-scale information technology projects, is one clear option to encourage sharing of expertise. GSA could enlarge its current small program to train procurement officers in ADP, or programs could be added through, for example, the Office of Personnel Management or the Department of Agriculture's Graduate School. Some of the private training/seminar organizations in the Washington area do address ADP procurement issues to some extent, although these often focus on the process from the vendor's perspective. GSA suggests that this enhanced training does not need to make procurement officers into computer experts, or ADP managers into procurement specialists, but simply needs to provide each with a layman's understanding of the other field. In helping these officials to develop the resourcefulness necessary to get through the procurement process successfully, it could be useful as part of the training to present a workshop on experiences with actual acquisitions, both effective and problematic, in order to give students an understanding of the team approach to acquisition, pitfalls to avoid, and possible innovations.[25]

---

[22] See, for example, two useful documents produced by the Institute for Computer Sciences and Technology: *Future Information Processing Technology 1983*, special publications No. 500-103, August 1983; and *Future Information Technology 1984: Telecommunications*, No. 500-119, December 1984.

[23] *A Five-Year Plan*, 1984, op. cit., p. 14.

[24] Eric Fredell, "White House Again Targets ICST," *Government Computer News*, Mar. 8, 1985.

One controversial option suggested by the Department of Commerce[26] is that Congress could experimentally exempt certain agencies (or parts of agencies) from the bulk of statutes and GSA rulings on procurement for a fixed period of time. Such an experiment could allow the agency to develop and try different techniques for acquiring information technology. Clearly, Congress would want to choose agencies whose track record in planning and procurement is already good, and both Congress and GSA should watch the experiment closely, while still allowing the agency flexibility. The outcome of such an experiment should be evaluated not just on the net cost to the government compared to more traditional procurement procedures, but on the effectiveness of the agency in using information technology to accomplish its mission.

Another interesting idea for sharing ADP expertise raised by Robert Head in his 1982 monograph is to establish the equivalent of a rapid-response troubleshooting team for information technology to help agencies plan for and implement major projects, either at the behest of the agency, OMB, or Congress. Head writes:[27]

> The computer SWAT team would be available to aid agency managers in planning major new projects to avoid potential schedule pitfalls. Work here might include the installation of SDLC [systems development life cycle] procedures to strengthen management control of large projects, the application of software engineering principles, assistance in specification writing, and the selection and supervision of outside contractors. This would be one key function.[28]
>
> The second function would be to enter into systems projects that have deteriorated to the point where the agency has obviously become unable to salvage them. In such situations those responsible for managing the project are typically defensive. In this case, the computer SWAT team could provide not only technical assistance but also a "damage assessment" by advising Congress and other concerned parties about the true nature of the project's difficulties.

OMB or GSA could develop such an interdisciplinary team and establish guidelines for their activities. The team would not necessarily be free-standing; rather it could be composed of experienced officials from other agencies who serve on a rotating or ad hoc basis.

Amendments to the Paperwork Reduction Act to provide a stronger and more detailed mandate for information technology planning and management in the executive branch.

OTA found that information technology planning warrants more specific attention both in legislation and oversight. A first step might be to consider strengthening and refining the planning requirement included in the Paperwork Reduction Act of 1980, with specific legislative guidance for the content of 5-year plans. Aside from mandating that the plan be updated each year, as proposed in the Paperwork Reduction Act Amendments of 1984 (and as is now the case, due to OMB's initiative), the guidance could specify that the plan include analysis of the impacts of information technology on the missions of the agencies, and on civil liberties and fair information practices.

---

[25] Francis McDonough, General Services Administration, letter to OTA, September 1985.

[26] Jimmie D. Brown, Director for Management and Information Systems, Department of Commerce, letter to OTA, Oct. 2, 1985.

[27] Robert Head, *Federal Information Systems Management*, op. cit., pp. 36-37; see also General Accounting Office, *Government-Wide Guidelines and Management Assistance Center Needed To Improve ADP Systems Development*, AFMD-81-20, Feb. 20, 1981.

[28] This kind of assistance is already available to agencies from GSA's Office of Software Development and Information Technology and the Federal Computer Performance Evaluation and Simulation Center (FEDSIM), which is under the auspices of the Air Force but performs contract services for other agencies.

Further, Congress may wish to examine in more detail current trends in the information available on information technology management, determine what kinds of information are vital to congressional oversight and agency decisionmaking, and request or direct the necessary information collection efforts. The Paperwork Reduction Act could, for example, require both a census of microcomputers and an inventory and description of major systems, and could require that GSA compile a more comprehensive report describing this information and the underlying trends. It would also be useful to establish some kind of inventory of software resources, since software has long since outstripped hardware in lifecycle cost and significance to programs.

OTA recognizes that, true to the IRM concept, there are costs associated with collecting such information. OMB and GSA officials, for example, have repeatedly expressed a hesitancy to collect further information because agencies already feel oppressed by the current information collection guidelines. In particular, agencies may resist providing information about microcomputers, since the unit cost is so low. Clearly, these arguments must be weighed against the potential value to Congress of having more complete and reliable information about trends in technology use.

Amendments to the Paperwork Reduction Act could also give individual agencies, in addition to OMB, a mandate for long-range planning. While agencies are currently required to plan, by OMB directives, a congressional mandate—and perhaps allocation of modest resources—may raise the visibility and effectiveness of the agency information technology planning process.

Other options would clarify the Paperwork Reduction Act's mandate for general information technology management. In the 98th Congress, several aspects of S. 2433 and H.R. 2718, proposed amendments to the Paperwork Reduction Act, would have clarified some of the definitions in the act, combined GSA's ADP and telecommunications funds, mandated that OMB's 5-year plan be updated annually, and specified further paperwork reductions. An effective congressional role in information technology management is difficult to construct, since there is a danger that Congress may be perceived as reaching too far into the management prerogatives of the executive branch. However, should Congress decide to take a more active role in this area, it could strengthen and expand the language of the Paperwork Reduction Act, setting forth goals for information technology management in order to define more specifically what is meant by IRM and what kinds of coordination and management structure the agencies should pursue. Such a congressional mandate may motivate quicker action by the agencies. While the act gives a very specific mandate for paperwork reduction, it gives only a bare minimum framework for information technology management.

Another possible option is to designate an additional assistant secretary for some agencies, whose primary responsibility would be information resources management. Since most agencies have designated their existing assistant secretary for administration as their senior official for IRM, many of these officials have been forced either to neglect IRM or to delegate the responsibilities. Establishing a new assistant secretary for IRM would ensure high-level visibility for the function, although it would also have clear costs in money and bureaucratic complexity. Such a new official also might have less authority than an assistant secretary for administration who also has jurisdiction over budgets, contracts, and facilities.

Chapter 4

Information Systems Security

Contents

Page
Summary 59

Introduction 60

Background 60
  Federal Information Security 62

Major Findings 67
  Finding 1 67
  Finding 2 69
  Finding 3 72
  Finding 4 75
  Finding 5 77

Appendix 4A.—Highlights of Information Security Policies of Selected Agencies 80

Appendix 4B.—Highlights of Findings on Information Vulnerability by the National Telecommunications and Information Administration 81

Tables

Table No. *Page*
4-1. Common Administrative, Physical, and Technical Information Security Measures 61
4-2. Illustrative ADP Security—Risk Assessment Questions 63
4-3. Key Federal Documents Affecting Information Systems Security 64
4-4. Committees Guiding the Implementation of NSDD 145 66
4-5. Selected GAO Reports Identifying Major Information Systems Security Problems, 1975-85 69
4-6. Systems Meeting GAO Criteria for Physical, Technical, and Administrative Security Safeguards 70
4-7. Systems Meeting GAO Criteria for Computer Security Management Evaluation 70
4-8. Security Techniques in Use by Federal Agencies in Unclassified But Sensitive Applications 71
4-9. Examples of Other Audits Identifying Significant Information Security Problems in Federal Agencies 71
4-10. Federal Agency Expenditures and Staffing for Computer and Communications Security 74

Chapter 4

Information Systems Security

SUMMARY

This chapter examines needs and policies for the protection of Federal data and information systems from a variety of problems, ranging from technical failures to unauthorized use or manipulation of data.

Concerns about the security of information systems began to become prominent in the mid to late 1960s, particularly in military and national security agencies of the government. Generally, while the Department of Defense (DOD), and particularly the National Security Agency (NSA), has developed a great deal of technical expertise in this area, the civilian agencies have lagged in awareness. In the last decade, however, concerns about both privacy and hackers have elevated the overall visibility of this issue.

The basic policy document for government-wide information security is the Office of Management and Budget's (OMB) Circular A-130 issued in December 1985 (replacing Circular A-71, Transmittal Memorandum No. 1, issued in 1978), which requires agencies to designate security officers, conduct risk analyses, and take other appropriate steps to protect their information systems. In September 1984, the White House issued National Security Decision Directive 145 (NSDD 145), which essentially attempts to bring together the separate paths of civilian and military information systems security, with NSA serving as a resource and coordinating point for all national security-related applications in the Federal Government. The scope of NSDD 145 and NSA's authority is based on a definition of "information sensitive for national security reasons" which has not yet been worked out, but is likely to be far broader than classified information alone.

OTA's major findings in this area are:

- The government faces fundamentally new levels of risks in information security because of increased use of networks, increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, and increased dependency on information technology overall.
- Although there has been some progress in the past 5 to 10 years, there is widespread evidence that Federal policy requiring the use of appropriate information systems security measures has been ineffective. The General Accounting Office (GAO) reports and the OTA Federal Agency Data Request indicate that agencies often are not taking the actions mandated by OMB Circulars A-71 and A-130, such as performing risk analyses and screening personnel who work with sensitive applications. For example, for systems that process sensitive but unclassified information, OTA found that about one-quarter of the agencies responding do not screen personnel, about one-half do not perform a management review of sensitive applications, and about 40 percent do not use audit software or restrictions on dial-up access for any of these systems. In addition, about 40 percent of agencies have not conducted a risk analysis in the last 5 years, about 75 percent do not have an explicit security policy for microcomputers, and about 60 percent do not have (and are not developing) contingency plans in the event of disruption of mainframe computers.
- Three key factors inhibit appropriate Federal information security measures: 1) competition for resources in Federal programs, which limits spending for a "latent" issue like security; 2) a lack of awareness or motivation among agency personnel and top management; and 3) an absence of clear guidance on appropriate security measures.

- As NSDD 145 is implemented, it becomes increasingly clear that NSA and the committees guiding its implementation will play a significant if not dominant role in all aspects of information security in the Federal Government, whether or not the information is classified. Thus, NSDD 145 is likely to result in stronger governmentwide leadership in information security policy; however, concerns have been expressed that it puts the national security community in an unusual influential, if not controlling, position on a key aspect of the Nation's information policy.
- Possible actions to improve Federal information systems security include: more intensive congressional oversight, changing budget procedures with information security receiving higher priority and visibility, designating a civilian agency to be responsible for security training and technical support in the nonmilitary sector of government, and revising and clarifying NSDD 145.

INTRODUCTION

This chapter and the next ("Chapter 5: Computer Crime") are closely tied, in that they both focus on the integrity of information systems, although they emphasize different aspects of the problem. There are four general kinds of measures to protect information systems: 1) technical measures, such as cryptography; 2) administrative measures, such as making sure disbursements cannot be authorized by only one person; 3) physical measures, such as locking up diskettes; and 4) legal remedies to discourage abuse and prosecute perpetrators. This chapter discusses primarily the technical, administrative, and physical security measures, while chapter 5 discusses computer crime legislation.[1]

Finally, though this chapter addresses information systems security considered broadly—including both computers and telecommunications—computer security is analyzed in more detail than telecommunications security. A related OTA study will provide further analysis of telecommunications security issues.[2]

---

[1] It should be noted that the management of information security is one important aspect of good overall information technology (or information resources) management. It is an axiom of the information technology management field that effective information security cannot be independent of other aspects of management, or relegated to technical security experts. Rather, the managers and users of information systems must consider security throughout the planning, implementation, and use of the systems. Thus, although this chapter focuses its analysis on one goal of information technology management—security—it should be emphasized that good overall management and good security practices are intertwined.

[2] The study, "New Communication Technologies: Implications for Privacy and Security," is scheduled for completion in fall winter 1986.

BACKGROUND

Attention began to focus on the security of unclassified information systems in the Federal Government in the mid to late 1960s. Important factors that led to this concern include the development of multi-user ("resource sharing") computer systems, and the growing interest in privacy and government data banks.[3] In addition, a number of notorious computer crimes in the 1970s reinforced the fact that information systems do indeed have significant vulnerabilities.[4]

---

[3] An important early document is a report by the Defense Science Board Task Force on Computer Security, "Security Controls for Computer Systems," edited by Willis H. Ware. It was originally issued in classified form in 1967, and later declassified and published for the Office of the Secretary of Defense by Rand Corp., Santa Monica, CA, 1979. For more historical information see also L.G. Becker, Congressional Research Service, "Computer Security: An Overview of National Concerns and Challenges," report No. 83-135 SPR, Feb. 3, 1983.

[4] See U.S. Department of Justice, Bureau of Justice Statistics, *Computer Crime: Computer Security Techniques*, September 1982. The document was prepared by SRI International under a contract with the Department of Justice.

The threats and problems faced by computer systems include:[5]

1. Mistakes, both errors and omissions, that result in loss of data integrity. Examples: keyboard entry errors, programming errors, bringing magnets near storage media.
2. Dishonest employees with self-serving goals (usually economic) committing acts they prefer not to be noticed. Examples: "Data diddling" to generate unauthorized disbursements; using privileged information for personal gains.
3. Loss or disruption to data-processing capability from any cause. Examples: fire, flood, hurricanes, civil unrest, falling aircraft (for computer installations near airports), and loss of supporting services and facilities.
4. Disgruntled employees who commit damaging acts without economic or other self-serving goals. Examples: employees accessing information after they quit; destroying essential tapes; or planting "logic bombs" of various sorts, which disrupt the computer's operating system at a specified time.
5. Outsiders who, through some illicit act, accidentally or intentionally cause loss of data integrity or loss of or disruption to the means of processing those data. Examples: hackers gaining unauthorized access and/or tampering with files, industrial espionage via eavesdropping on data transmissions.

Table 4-1.—Common Administrative, Physical, and Technical Information Security Measures

Administrative security measures:
- Background checks for key computer employees.
- Requiring authority of two employees for disbursements.
- Requiring that employees change passwords every few months, do not use the names of relatives or friends, and do not post their passwords in their offices.
- Removing the passwords of terminated employees quickly.
- Providing security training and awareness programs.
- Establishing backup and contingency plans for disasters, loss of telecommunications support, etc.
- Storing copies of critical data off-site.
- Designating security officers for information systems.
- Developing a security policy, including criteria for sensitivity of data.
- Providing visible upper management support for security.

Physical security measures:
- Locking up diskettes and/or the room in which microcomputers are located.
- Key locks for microcomputers, especially those with hard disk drives.
- Requiring special badges for entry to computer room.
- Protecting computer rooms from fire, water leakage, power outages.
- Not locating major computer systems near airports, loading docks, flood or earthquake zones.

Technical security measures:
- Audit programs that log activity on computer systems.
- Security control systems that allow different layers of access for different sensitivities of data (e.g., each level requires a different password).
- Encrypting data when it is stored or transmitted, or using an encryption code to authenticate electronic transactions.
- Techniques for user identification, ranging from simple ones such as magnetic stripe cards to more esoteric "biometric" techniques, which rely on hand or eye scanners (just beginning to be used).
- "Kernel"-based operating systems, which have a central core of software that is tamperproof and controls access within the system.[a]
- "Tempest" shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment.[a]

[a] Generally used only in military or other national security applications.

SOURCE: Office of Technology Assessment.

Table 4-1 lists some of the common measures that can be used to protect information systems from these problems. It is not exhaustive, but suggests the range of safeguards that are available. In order to match the value of data and the differing risks with appropriate safeguards, information security experts commonly use a technique known as risk analysis. It is a variant of risk analysis techniques that have gained prominence in the last two decades to help make decisions about environmental issues and other technological hazards.[6] In general, a risk analysis for an information system involves answering the following questions:

---

[5] Adapted from Robert H. Courtney, Jr., and Mary Anne Todd, "Problem Definition: An Essential Prerequisite to the Implementation of Security Measures," paper prepared for presentation to the Second International Congress and Exhibition on Computer Security, Toronto, Sept. 10-12, 1984, p. 4. Courtney argues that these problems are listed in order of decreasing economic importance—i.e., that mistakes are the most important problem, and outsiders the least—although others would rank the problems differently.

[6] The National Science Foundation's Technology Assessment and Risk Analysis Program has funded and coordinated much of the pioneering work in this area. See, for example, V. Covello and M. Abernathy, "Risk Analysis and Technological Hazards: A Policy-Related Bibliography," National Science Foundation (mimeograph), 1982; National Research Council, Committee on Risk and Decision Making, *Risk and Decision Making: Perspectives and Research* (Washington, DC: National Academy Press, 1982).

1. What are the threats or vulnerabilities that this system faces?
2. How likely are those threats or vulnerabilities?
3. What would be lost?
4. What are the alternatives for protecting against these threats, and how does the cost of the alternatives compare with the size and likelihood of losses if the system is not protected?

OMB's Circular A-130 (and its predecessor, Circular A-71, Transmittal Memorandum No. 1) requires risk assessments for information systems at least every 5 years, although it does not specify what constitutes a risk assessment or an information system. Risk analysis techniques for information systems range from an informal and brief qualitative procedure for a small microcomputer system, to a highly quantitative, in-depth examination of a major computing center. The latter are typically performed by a consultant for $50,000 to $250,000 and up. In the past few years, several vendors and research labs have developed risk analysis procedures that are automated and can be considerably cheaper.[7]

A risk analysis technique published by the National Bureau of Standards (NBS) in 1979 is the basis of many risk analyses performed in government and in the private sector. The procedure, published in Federal Information Processing Standards Publication 65, involves identifying potential threats, and then developing an "annualized loss expectancy" for each threat. For example, one might estimate that a fire in the tape storage room would cause $300,000 in losses (e.g., including damage, denial of use, and possible disclosure), that it would occur (within an order of magnitude) once every 30 years, and that the resultant annualized loss estimate was $10,000 (i.e., $300,000/30). Once annualized loss estimates are determined using this system, one can compare them to the costs of implementing protective measures. For example, the cost for a fire control system for the tape storage room, amortized over its expected lifetime, might be $5,000 per year. If so, the analysis would suggest that such a system ought to be considered.

Although risk analyses modeled on the NBS system are widely used, they have distinct drawbacks. In particular, the process can become quite lengthy and include a great deal of personal judgment. Many critics have noted, for example, that estimating the frequency of events that have never occurred is particularly difficult. Thus, simpler and less quantitative techniques for risk analysis are becoming more popular, especially for smaller information systems. The U.S. Geological Survey (USGS), for example, uses a questionnaire-based system to identify possible risks and to determine whether appropriate protective measures have been considered. Table 4-2 provides an example of the format. The principle behind the USGS system is to identify a set of baseline measures and to ensure that system managers have considered implementing them. They are thus informed and accountable for the security of their systems.

Federal Information Security

Though there are common aspects, there is wide variation among and within Federal agencies in the kinds of information technology they use, in the nature of their information security problems, and in their awareness of those problems. Even within agencies (e.g., DOD), different functions or installations will range from being at the cutting edge of sophistication in information security to very minimal awareness and protective measures. And clearly, the national security community is distinctly different from much of the rest of government in the threats it faces and in its sophistication with regard to computer security.

Largely because of this difference in sophistication, the military (including parts of civilian government that generate classified infor-

---

[7] See, for example, Suzanne Smith and J.J. Lim, Los Alamos National Laboratory, "A Framework for Generating Automated Risk Analysis Expert Systems," presentation at Federal Information Systems Risk Analysis Workshop, Montgomery, AL, Jan. 22, 1985.

Table 4-2.—Illustrative ADP Security—Risk Assessment Questions

Site location

Controls and procedures	Yes	Risk is acceptable	Corrective action
1. Has the responsibility for the protection of each and every ADP resource (computer system, data, programs, etc.) been explicitly assigned?			
2. Are procedures in place to inform employees what resources they are expected to protect and from what hazards, what variances they are to note, and what corrective action they are to take?			
3. Are procedures in place to ensure the timely and complete separation of terminated employees?			
4. Is there a policy consistent with generally accepted practice about who may access and update data?			
5. Where indicated by the sensitivity of the resource and size of user population, is the policy enforced by the system?			
6. Is each individual user of the system uniquely identified?			
7. Is there a procedure (e.g., password, magnetic-stripe card) to authenticate the identity of the individual user of the system?			
8. Are users restricted to only those resources (e.g., data sets, records or segments, fields, transactions, etc.) required for their job?			

SOURCE: U.S. Geological Survey

mation) and civilian sides of government have taken different paths in responding to escalating security concerns. The military side has been pursuing information security (particularly telecommunications, but increasingly computer security also) for much longer than other parts of government. It has powerful institutions and a great deal of technical expertise in this area.[8] Much of this expertise has traditionally been centered in NSA, whose mission includes both gathering intelligence from international telecommunications transmissions, and protecting U.S. transmissions from interception, alteration, and disruption.

Beginning in the 1970s, the concern on the military side broadened into several major programs and Presidential directives for protecting national security information. A key milestone was President Carter's Presidential Directive/National Security Council-24 (PD-24), issued on February 16, 1979. The directive focused on developing telecommunications security safeguards for classified information as well as unclassified government and private sector information that would be "useful to an adversary." It gave joint responsibility to the Secretary of Defense (delegated to NSA) and to the Secretary of Commerce (delegated to the National Telecommunications and Information Administration (NTIA)) to monitor telecommunications security needs in government and the private sector, and to propose a national policy for cryptography.[9] Eventually, NTIA's role in information security was phased out during the Reagan Administration.

For unclassified information unrelated to national security, the motivations for addressing information security are quite different.

---

[8] See Sanford Sherizen, "Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options," OTA contractor report, February 1985.

[9] Presidential Directive/National Security Council-24 (unclassified extract), "National Telecommunications Protection Policy," Feb. 16, 1979.

Rather than facing a sophisticated adversary who seeks to obtain protected information, civilian agencies (and many parts of the military agencies as well) face a diffuse set of problems, ranging from computer-related embezzlement of funds by employees to unauthorized use of sensitive personal or proprietary data, to simple errors and omissions. The pattern of policy development for protection of this kind of information has been similarly diffuse. In the late 1960s and early 1970s, congressional concerns about privacy led to the Privacy Act of 1974, which controls the collection and use of personal information by Federal agencies.

One of the most significant policy actions for governmentwide information security took place in 1978, when OMB issued Transmittal Memorandum #1 (TM-1) to its Circular A-71 on the management of Federal information technology. TM-1 requires agencies to implement a computer security program. This program includes: 1) designating a security officer for each installation, 2) establishing personnel screening procedures for those who work with sensitive computer systems, 3) establishing procedures for evaluating the sensitivity of applications and certifying that systems are appropriately secure, 4) performing periodic audits and risk analyses for each computer installation, and 5) establishing contingency plans for disruptions to information systems. The memorandum also assigns to Federal agency heads the responsibility for assuring appropriate levels of security in their information systems; and it directs the General Services Administration (GSA) and NBS to develop policy guidelines and standards for Federal information systems security.

Table 4-3 highlights the policy documents that represent the current policy framework for information systems security. In addition, individual agencies, particularly DOD and intelligence agencies, have information security policies that go beyond the governmentwide guidelines. See appendix 4A at the end of this chapter for some examples.

Table 4-3.—Key Federal Policy Documents Affecting Information Systems Security

Brooks Act of 1965 (Public Law 89-306):

Gives OMB and GSA joint authority to set policy on Federal information technology; Commerce/NBS provides supporting standards, research, and technical assistance.

Privacy Act of 1974 (Public Law 93-579):

Restricts collection and use of personal information by agencies; requires them to take precautions to prevent unintended disclosure of personal information.

OMB Circular A-71, Transmittal Memorandum #1, 1978:

Requires agencies to establish a computer security program, including periodic risk analyses, management certification of sensitive applications, and designation of computer security officers.

Presidential Directive/National Security Council-24 (PD-24), "National Telecommunications Protection Policy," Feb. 16, 1979 (superseded by NSDD 145):

Gives Defense/NSA and Commerce/NTIA joint responsibility to monitor telecommunications security needs in government and private sector, and to propose cryptography policy. NTIA's role was ultimately phased out.

Paperwork Reduction Act of 1980 (Public Law 96-511):

Endorses the concept of information resources management, establishes the Office of Information and Regulatory Affairs at OMB, and charges that office with evaluating agency information management and setting and coordinating related policies.

Federal Managers Financial Integrity Act of 1982 Public Law 97-255):

Requires agencies to examine their internal control systems and report deficiencies and plans for correcting those deficiencies to the President and Congress.

National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," issued by the White House, Sept. 17, 1984:

Sets NSA as the focal point for both military and civilian information security related to national security. NSA is to assist an interagency committee (NTISSC) in developing and coordinating policies, evaluating computer and telecommunications security, and reviewing and (for telecommunications) approving budgets for computer and communications security efforts throughout government.

OMB Circular A-130, "Management of Federal Information Resources" Dec. 12, 1985 (supersedes A-71):

Reinforces provisions of A-71, updates A-71 to acknowledge microcomputers, Federal Managers' Financial Integrity Act, NSDD 145.

SOURCE: Office of Technology Assessment

Since the early 1980s, there has been a resurgence of interest in information security problems and policies, both for national security-related and other Federal systems. Some of this interest is clearly tied to the recent incidents of computer "hackers" gaining unauthorized access to computer systems, ranging from the Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory. Although hackers have often brought attention to computer security issues, they appear to be only a small part of the overall computer security problem. Security experts are nearly unanimous in their view that the more significant security problem is abuse of information systems by those authorized to use them, rather than by those trying to penetrate the systems from outside.[10] (See ch. 5 for further discussion of computer crime.)

Other factors that have contributed to renewed interest in information systems security in the 1980s include a growing awareness of the Federal Government's dependence on information technology, and an increasing sense that existing policy in this area is inadequate. For example, a 1982 GAO report said that Circular A-71 has not been implemented effectively because it failed to: 1) provide clear guidance to agencies on minimum safeguards needed, 2) clarify the relationship between measures for national security information and measures for other kinds of information, and 3) provide guidance on telecommunications security.[11]

In part as a result of this renewed interest and controversy over information systems security policies, the executive branch has taken two very significant steps to change these policies. The first was NSDD 145, issued by the President on September 17, 1984, which gives the NSA new authorities and responsibilities for a wide range of military and nonmilitary information security functions. It is to "act as the government focal point for cryptography, telecommunication systems security, and automated systems security." This aspect of NSDD 145 is unusual and worthy of attention—essentially, the directive aims to bring together the separate paths of military and civilian agencies in national security-related information security, and put them both under the guidance of NSA.

NSA's role in this respect will be guided by two interagency committees. One is the the Systems Security Steering Group, a high-level oversight group that meets twice a year. The second is a working group known as the National Telecommunications and Information Systems Security Committee (NTISSC), composed of 22 agency representatives, 12 from the national security community.[12] See table 4-4 for the membership of these committees. NTISSC meets quarterly, and has subcommittees on automated information systems security and telecommunications security that meet more frequently.

The scope of the roles of NSA and NTISSC depends on their interpretation of their mandate to assist in protecting information "the loss of which could adversely affect the national security interest." The extent to which this category includes unclassified information (essentially establishing a fourth level of classification beyond the "top secret," "secret," and "confidential" designations now used) will determine the range of military and civilian agency activities that will be influenced by NSDD 145.

---

[10] See, for example, Joel Zimmerman, "The Human Side of Computer Security," *Computer Security Journal*, summer 1984, pp. 7-19. The relative importance of "outsiders" penetrating information systems is viewed by some as a critical difference between military and civilian information systems. Because personnel running military systems have usually been more carefully "cleared" than those in civil agencies, and because the potential adversaries seeking national security information are much more sophisticated, military computer security experts often emphasize protection from outside penetration. See "Computer Security, The Defense Department, and the Private Sector—A 3-Part Dialogue About Fundamental Objectives and Needs," in the journal referenced above, pp. 53-66. The differences between military and civilian information security needs will be a continuing theme throughout this chapter.

[11] U.S. General Accounting Office, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices*, MASAD-82-18, Apr. 21, 1982.

[12] The extent to which NTISSC is "dominated by the military" became an issue in hearings held by the House Science and Technology Subcommittee on Transportation, Aviation, and Materials, June 27, 1985. The U.S. General Accounting Office, in its testimony, indicated that 10 of the 22 representatives are from defense agencies (the Secretary of Defense; the Joint Chiefs of Staff; the Army, Navy, Air Force, and Marine Corps; the Defense Intelligence Agency; the National Security Agency; the National Communications System; and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence). Perhaps more important than the number of defense agency representatives is the number of representatives whose primary concern is the protection of classified information, since the needs and motivations of such representatives are significantly different from those of other agencies. Under this criteria it would make sense to add the Director of Central Intelligence, and the Assistant to the President for National Security Affairs, making 12 of 22 committee members from the "national security community," considered broadly.

Table 4-4.—Committees Guiding the Implementation of NSDD 145

Systems Security Steering Group:

1. Secretary of State
2. Secretary of the Treasury
3. Secretary of Defense[a]
4. Attorney General
5. Director of OMB
6. Director of Central Intelligence[a]
7. Assistant to the President for National Security Affairs, chair[a]

National Telecommunications and Information Systems Security Committee:

Consists of a voting representative of each of the above, plus a representative designated by each of the following:

8. Secretary of Commerce
9. Secretary of Transportation
10. Secretary of Energy
11. Chairman, Joint Chiefs of Staff[a]
12. Administrator, GSA
13. Director, FBI
14. Director, Federal Emergency Management Agency
15. Chief of Staff, Army[a]
16. Chief of Naval Operations[a]
17. Chief of Staff, Air Force[a]
18. Commandant, Marine Corps[a]
19. Director, Defense Intelligence Agency[a]
20. Director, National Security Agency[a]
21. Manager, National Communications System[a]
22. Assistant Secretary of Defense for Command, Control, Communications and Intelligence, chair[a]

[a] Denotes a representative closely associated with the defense/national security community. See footnote 12, in text.

SOURCE: National Security Decision Directive 145, unclassified version, "National Policy on Telecommunications and Automated Information System Security," issued by the President, Sept. 17, 1984.

The directive is still early in its implementation. NTISSC and its related subcommittees have begun to meet (on a classified basis) to work out the implementation of the directive. They have developed a report on the status of computer and telecommunications security in the government, again classified, although OTA obtained an unclassified extract, discussed below. Some of the other early activities of the NTISSC and its subcommittees include working on a scheme for categorizing sensitive, but unclassified, information in both the military and civilian agencies. They have also developed an OMB bulletin (No. 85-11) that asks agencies to report information to OMB on information security measures for classified systems. NSDD 145 will be discussed in more detail later in this chapter.

The second major recent policy action on information systems security is a new OMB circular, A-130, "Management of Federal Information Resources," that supersedes and revises A-71 and three other circulars.[13] The revision attempts to present integrated guidance on Federal Information Resources Management, considered broadly. The new circular does not make major changes to A-71, but rather strengthens and clarifies it in a number of areas:

- It defines security as "both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more . . . . security of information systems is first and foremost a management issue and only secondly a technical problem of computer security."
- It emphasizes new vulnerabilities in the government as a result of "smaller and more powerful computer systems and new communications technology and transmission media, together with the greater involvement of end users in managing information resources."
- It acknowledges the relationship between the former Circular A-71 and Circular A-123, "Internal Control," by noting that agencies should consider information security an essential part of their internal control reviews.[14]
- It expands and clarifies the definition of "sensitive data" to include "data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, rec-

---

[13] The other circulars are A-90 ("Cooperating With State and Local Governments to Coordinate and Improve Information Systems"), A-108 ("Responsibilities for the Maintenance of Records About Individuals by Federal Agencies"), and A-121 ("Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities").

[14] In 1983, the Office of Management and Budget revised Circular A-123, which, along with the Federal Managers Financial Integrity Act (Public Law 97-255), requires agency heads to analyze safeguards and audit systems (of all kinds, including those applying to information systems), and report to the President and Congress annually with a plan for correcting any weaknesses. A U.S. General Accounting Office review of the first-year implementation of the Financial Integrity Act said that internal controls related to information systems received inadequate coverage in the reviews, and that some agencies were uncertain of the relationship between A-71 and A-123.

ords about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act."[15]

- It reasserts the need for agencies to define security needs before procuring or starting formal development of application systems.
- It adapts its requirement for risk analyses for all systems to note that "risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system."
- It requires agencies to establish a security awareness and training program.
- It briefly acknowledges that the Secretary of Defense has a role in information systems security for systems that process "information the loss of which could adversely affect the national security interest," and directs DOD to provide technical material and assistance to Federal agencies on information systems security.[16]

MAJOR FINDINGS

Finding 1

The Federal Government faces fundamentally new levels of risks in information security because of increased use of networks, increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, and increased dependency on information technology overall.

This finding provides an important foundation for assessing the importance of information systems security as an issue. These trends are also discussed in several other chapters in this report.

Increased Use of Networks

Computer power is becoming cheaper and more widely distributed and the machines are becoming more sophisticated in their capabilities to share data and communicate with one another. As a result, the use of networks of all kinds, from local area networks linking an office's personal computers to dedicated data networks spanning thousands of miles, is expanding rapidly. In addition, an increasing number of computers are accessible via dial-up connections using ordinary phone lines. While these linkages add to the effectiveness of information technology systems, they also raise new vulnerabilities by allowing possible abuses at a distance, and by increasing opportunities for eavesdropping.[17]

Increased Computer Literacy

The simple fact that more people know how to use computers, and that computers are becoming easier to use, means that there are more people both inside and outside the Federal Government who have the skills to use information systems for unintended purposes.

---

[15] The definition of sensitive data proposed in the draft circular is quite different from the concept of sensitive data in NSDD 145, which considers data sensitive if it is related to national security; the exact definition for NSDD 145 is yet to be released, as will be discussed later in this chapter.

[16] NSDD 145 required that the Office of Management and Budget review A-71, Transmittal Memorandum #1, and amend it as appropriate for consistency with the directive. Although Circular A-130 states that it has satisfied this requirement (appendix IV, section 2), it has done so only in a *pro forma* manner. On closer inspection, the wording in the circular actually does very little to clarify the substantial confusion about the relative roles of NTISSC, NSA, NBS, OMB, GSA, and other agencies in the area of information security.

[17] OTA's forthcoming study, "New Communication Technologies: Implications for Privacy and Security," will discuss these issues further. Also see U.S. General Accounting Office, *Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies*, LCD-81-1, Nov. 12, 1980; and U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, OTA-CIT-29 (Washington, DC: U.S. Government Printing Office, October 1985).

Microcomputers, Workstations, and Decentralized Data Processing

As discussed in chapter 2, the Federal Government is in the midst of an explosion in microcomputer use, from almost none in 1975 to estimates of over 100,000 in 1985. In addition to their use as independent data processors, microcomputers that are used as "intelligent workstations"[18] to exchange data with a larger computer and manipulate it independently raise very significant managerial issues. This decentralization of data-processing capabilities reduces the degree of management control over data and information systems use; it increases the number of people using information systems; and these machines have new security problems of their own. On the other hand, decentralized systems can be more secure in some ways because all data are not vulnerable as they would be in one large system.

In essence, designers and users of large-scale computers were just beginning to understand information security needs and implement effective measures when the microcomputer appeared on the scene, destroying the fragile developing consensus about security. Westin and Hoffman[19] describe seven key risks particularly applicable to microcomputers:

1. lack of clear organizational policy identifying sensitive information on office automation systems;
2. failure to provide adequate physical-location security for machines and storage media;
3. failure to have key locks on terminals;
4. weaknesses in password systems governing access to central databases from microcomputers;
5. frequent lack of access logs or journals on office systems of connected microcomputers;
6. absence of methods to record efforts to penetrate security of office-based microcomputer systems; and
7. absence of either security education for end users or auditing of user practices.

Other problems include the generally simplistic (and thus hard to protect) architectures of small computer systems, lack of adequate off-site backup for data in small computers, and reluctance of management to demand security discipline from users of small computers.

Management guidelines need to be developed in each of these areas in order to maintain information security. Only 27 percent (37 out of 139) of agencies responding to OTA's Federal Agency Data Request indicated that they had an explicit information security policy for microcomputers.

NBS has attempted to help agencies develop such policies with a recent publication, *Security of Personal Computer Systems: A Management Guide*, January 1985. Nevertheless, there is likely to be some lag between the rapid increase in microcomputer use and the development and implementation of effective administrative measures. An example of such a lag is the fact that the main GSA retail microcomputer store, Office Technology Plus, does not carry any security-related hardware or software; they refer inquiries to their store near the Pentagon.[20] Security is not yet considered an integral part of the world of most microcomputer vendors and users. This situation points to the need for greatly increased vigilance on the part of information system managers and users.

Increased Dependency on Information Technology

As noted in chapter 2, Federal expenditures for information technology have increased significantly, from $10.4 billion in fiscal year 1983 to an estimated $15.2 billion in fiscal year 1986. In addition to using more information technology for traditionally automated applications (e.g., payroll processing), the government is using information technology in a variety of other areas, including decision support, reporting and dissemination of information, and auditing. Many Federal missions, from social welfare programs to revenue collection to air traffic control, are critically dependent on information technology. This escalating intensity and range of use reinforces the importance of effective safeguards and policies regarding privacy and security. Further, in the next decade there will increasingly be new information technologies—such as voice data input/output, digital telephone networks, optical storage of data, and expert systems—with different security problems.

---

[18] The term "intelligent workstation" is used by computing experts to refer to a computer terminal that has substantial stand-alone processing capabilities, as opposed to a "dumb terminal," which can only be used to communicate with a shared larger computer.

[19] Alan Westin and Lance Hoffman, "Privacy and Security Issues in the Use of Personal Information About Clients and Customers on Micro and Personal Computers Used in Office Automation," OTA contractor report, February 1985.

[20] OTA site visit, Office Technology Plus, March 1985; telephone conversation with Ken Jones of OTP, February 1986.

Together, these trends imply that the whole area of information systems security is in flux and the potential problems are perhaps an order of magnitude greater than they were a decade ago. These new levels of risk, along with the major policy changes in the executive branch, suggest the need for increased congressional attention in this area.

Finding 2

Although there has been some progress in the past 5 to 10 years, there is widespread evidence that Federal policy requiring the use of appropriate information systems security measures has been ineffective.

There is substantial evidence pointing to continuing (and perhaps worsening) information security problems in the Federal Government. The evidence comes principally from five sources—GAO reports, OTA's Federal Agency Data Request, other audits, congressional hearings and studies, and expert opinion.

GAO Reports

Table 4-5 lists some of the GAO reports over the past decade that have been critical of information security practices in Federal agencies. These reports range from audits of specific agencies, such as the Social Security Administration or the Financial Management Service, to broader studies critical of governmentwide practices. GAO's 1982 study, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices*, mentioned earlier, argued that OMB's policy in A-71 was never clear enough, it did not establish minimum standards, and agency performance was not reviewed for compliance.

Table 4-5.—Selected GAO Reports Identifying Major Information Systems Security Problems, 1975-85

General:

Computer-Related Crimes in Federal Programs, Apr. 27, 1976, FGMSD-76-27.

Fraud in Government Programs: How Extensive Is It and How Can It Be Controlled? Sept. 30, 1981, AFMD-81-73.

Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, Apr. 21, 1982, MASAD-82-16.

Computers and data processing:

Managers Need To Provide Better Protection for Federal Automatic Data Processing Facilities, May 10, 1976, FGMSD-76-40.

Automated Systems Security—Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data, Jan. 23, 1979, LCD-78-123.

Central Agencies Compliance With OMB Circular A-71, Transmittal Memorandum No. 1, Apr. 30, 1980, LCD-80-56-I.

Most Federal Agencies Have Done Little Planning for ADP Disasters, Dec. 18, 1980, AFMD-81-16.

Telecommunications:

Vulnerabilities of Telecommunications Systems to Unauthorized Use, Mar. 31, 1977, LCD-77-102.

Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies, Nov. 12, 1980, LCD-81-1.

Audits of specific agencies:

IRS' Security Program Requires Improvements To Protect Confidentiality of Income Tax Information, July 11, 1977, GGD-77-44.

Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments, Aug. 9, 1979, HRD-79-104.

The Bureau of the Census Must Solve ADP Acquisition and Security Problems, Oct. 31, 1981, AFMD-82-13.

Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed, Dec. 10, 1981, HRD-82-19.

Weak Financial Controls Make the Community Services Administration Vulnerable to Fraud and Abuse, Aug. 22, 1980, FGMSD-80-73.

Improvements Needed in General Automated Data Processing Controls at the National Finance Center, July 12, 1985, AFMD-85-38.

SOURCE: Office of Technology Assessment.

GAO has conducted a survey of information security practices at key computer installations of 17 Federal agencies. The results, summarized in tables 4-6 and 4-7, show that only

Table 4-6.—Systems Meeting GAO Criteria for Physical, Technical, and Administrative Security Safeguards

	Number of systems having safeguards
Physical safeguards:	
Physical perimeter	16
Entry by badge or cypher lock	24
Use of security guards	22
Use of smoke and/or heat detectors	24
Technical safeguards:	
Identification and authentication	23
Audit trails or logs	10
Discretionary access controls (authorization)	24
Administrative safeguards:	
Separation of duties	15
Physical, administrative, and technical procedures tested	20
Audit trail information reviewed	10
Passwords required to be changed	21
Have all safeguards	5[a]

[a] Although these systems contained all evaluated safeguards, they may still be vulnerable because: 1) GAO evaluated selected safeguards only, and 2) all evaluated management responsibilities were not implemented. GAO does not know how vulnerable the systems may be because this survey did not involve testing the effectiveness of the safeguards.

NOTE: Total number of systems examined = 25.

SOURCE: Statement of William Franklin, Associate Director, IMTEC Division, General Accounting Office, before the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, "Automated Information Systems Security in Federal Civil Agencies," Oct. 29, 1985.

Table 4-7.—Systems Meeting GAO Criteria for Computer Security Management Evaluation

Management responsibilities	Number of systems meeting requirements
Risk management	8
Training	2
ADP personnel security	2
Assigned responsibility	4
Budgeting and accounting for security cost	1
Contingency plans (exist and tested)	9
Independent evaluation or audit	19
Written procedures	11

NOTE: Total number of systems examined = 25.

SOURCE: Statement of William Franklin, Associate Director, IMTEC Division, General Accounting Office, before the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, "Automated Information Systems Security in Federal Civil Agencies," Oct. 29, 1985.

5 of these 25 critical systems had all appropriate safeguards. Two areas in which a majority of systems fell short were:

1. the use of audit logs to monitor system activity; and
2. management responsibilities, including provisions for effective training, personnel security, assignment of responsibilities, budgeting and accounting for security cost, proper contingency plans, and available written security procedures.

OTA's Federal Agency Data Request

Table 4-8 shows the percentage of Federal agency components that reported using a variety of information security techniques for sensitive, unclassified information. Only 34 percent of agencies reported that they have screened all of their sensitive, unclassified computer applications for sensitivity and appropriate safeguards before use, and only 61 percent report using personnel screening for all of these applications. Both of these measures are mandated by A-71/TM-1, and by the new circular, A-130. In addition, only 78 of 134 (58 percent) agencies reported that they had conducted one or more risk analyses in the last 5 years, a procedure also mandated by OMB's guidance. Finally, only 57 percent of agencies reported that they had (or were in the process of developing) contingency plans to handle the disruption of their major mainframe computers. The agencies did report significant use of passwords, backup of key data files, and physical security for hardware, although only 58 percent reported that they used audit software to monitor the activities on systems processing sensitive, unclassified information.

Other Audits

Reports by the agencies' own inspectors general, and by the agencies' upper management under the Federal Managers Financial Integrity Act, also frequently identify weaknesses—many of them long-standing—in control procedures related to information security. See table 4-9 for examples. A GAO review of agencies' internal control reports submitted under the Federal Managers Financial Integrity Act indicated that the number of agencies reporting material weaknesses in automatic data processing controls rose from 10 in 1983 to 14 in 1984 (out of a total of 18 of the largest agencies).[21] In addition, the Na-

---

[21] U.S. General Accounting Office, *Financial Integrity Act: The Government Faces Serious Internal Control and Accounting Systems Problems*, December 1985.

Table 4-8.—Security Techniques in Use by Federal Agencies in Unclassified But Sensitive Applications

Technique	Number of components using	Percent	Number reporting use for 100% of systems	Percent
Applications screening	67	48.2%	47	33.8%
Personnel screening	102	73.4	85	61.2
Audit software	80	57.6	30	21.6
Restrictions on dial-up access	85	61.2	65	46.8
Password controls	133	95.7	106	76.3
Encryption	30	21.6	9	6.5
Backup hardware	87	62.6	48	34.5
Backup of key data files	133	95.7	110	79.1
Physical security for hardware	127	91.4	94	67.6
Other	9	6.5	5	3.6

NOTE: Total agency components responding = 139.

SOURCE: OTA Federal Agency Data Request.

Table 4-9.—Examples of Other Audits Identifying Significant Information Security Problems in Federal Agencies

Department of Energy, Inspector General, "Screening Contractor Employees Having Access to Sensitive, Unclassified Data Contained in Departmental Computer Systems," Oct. 20, 1981, MR 81-44.

General Services Administration, Inspector General, "Insufficient Controls and Policies Exist To Effectively Procure, Manage, and Use Microcomputer Assets," Region 10, undated, A40349/10/F/840926.

Agency for International Development, Auditor General, "Survey of Computer Security for AID's Washington Based Automated Information System," Dec. 24, 1980, 81-26.

Department of the Interior, Inspector General, "Synopsis of Recent ADP Audit Findings," February 1985, H-MO-MOA-06-85(a).

Agencies listing ADP security flaws in their reports under the Federal Managers Financial Integrity Act:

Department of Education
Department of Commerce
Nuclear Regulatory Commission
Department of Health and Human Services—Health Care Financing Administration, Public Health Service
General Services Administration
Department of Agriculture
Department of Housing and Urban Development
Department of the Treasury
Office of Personnel Management
Department of Labor
Veterans Administration
Small Business Administration
National Aeronautics and Space Administration
Environmental Protection Agency
Department of State
White House
Department of Defense

SOURCE: Office of Technology Assessment, various agency reports.

tional Telecommunications and Information Administration, as part of its duties under PD-24, discussed earlier, performed 28 surveys of telecommunications and information vulnerability in civilian agencies during 1979 to 1984, involving interviews and briefings with hundreds of agency staff. A summary of the findings from the first 21 surveys is presented in appendix 4B at the end of this chapter, and indicates significant problems in the area of telecommunication security in particular.

Finally, the first annual report from the NTISSC (mandated by NSDD 145) describes the government's posture in information systems security as "poor and rapidly getting worse," and in communications security as "unsatisfactory." The report recommends, in part, that the government develop a coherent framework for computer security policies, and that such policies require each system processing classified or sensitive data to have a personal identification and authentication system, audit trails that keep a record of activity, a designated security officer, a written security plan, control over physical access, and security controls on removable storage media. The report also calls for cabinet-level action to increase manpower and funding in computer and communications security governmentwide.[22]

See chapter 5 for further studies of computer crime in the Federal Government.

Congressional Studies and Hearings

Several congressional committees have played a key role in evaluating the state of information security in the Federal Government. Two reports in the mid-1970s by the Senate Committee on Government Operations (now Governmental Affairs), then chaired by Senator Abraham Ribicoff, noted widespread computer security problems and urged improved coordination in policy regarding computer security and abuse.[23] A 1983 report from the same committee, now chaired by Senator William Roth, also highlighted some of the same issues and concerns.[24]

---

[22] National Telecommunications and Information Systems Security Committee, "First Annual Evaluation of the Status of Telecommunications and Automated Information Systems Security in the United States Government," Aug. 10, 1985 (unclassified extract).

On the House side, the Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, formerly chaired by Representative Dan Glickman, has held a series of hearings on computer and telecommunications security, and has issued a report urging more leadership in security policy, more Federal research and development and educational programs in computer security, and the establishment of a national commission on information security and policy issues.[25] The House Committee on Government Operations has also held hearings, particularly on the role of NSA and NSDD 145.[26]

Expert Opinion

Based on OTA's workshops and other contacts with Federal information technology managers, most information security officials agree that there are serious, continuing security problems. While many officials would assert that there has been some improvement in the past few years as Federal personnel have become more aware of security issues (mostly through publicity about hackers), they would also acknowledge that frequently there is a lack of attention to information security on the civilian side of government. OMB staff, for their part, openly acknowledge that A-71/TM-1 has not been effective, and this realization is one of the motivations for revising that circular and incorporating it into the new circular on Federal information resources management.

Finding 3

Three key factors inhibit appropriate Federal information security measures:

1. **competition for resources in Federal programs, which tends to limit spending for a "latent" issue like security;**
2. **a lack of awareness or motivation among agency personnel; and**
3. **an absence of clear guidance on appropriate security measures.**

While there are many and varied reasons for the lack of attention paid to information security among Federal programs, these three factors seem to be common themes mentioned frequently in conferences, personal contacts, and workshops with Federal agency staff.[27]

---

[23] Senate Committee on Government Operations, *Problems Associated With Computer Technology in Federal Programs and Private Industry: Computer Abuses*, 94th Cong., 2d sess., 1976; and *Computer Security in Federal Programs*, 95th Cong., 1st sess., 1977.

[24] Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Federal Computer Security: An Analysis of Congressional Initiatives and Executive Branch Responsibilities* (prepared by the Congressional Research Service), 98th Cong., 1st sess., 1983.

[25] House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, hearings on "Computer and Communications Security and Privacy," Sept. 26, Oct. 17, and Oct. 24, 1983, and Sept. 24, 1984; and report, *Computer and Communications Security and Privacy*, April 1984. The Subcommittee has also held hearings evaluating National Security Decision Directive 145, June 27, 1985. These will be discussed in more detail later in the chapter. Finally, both the House and Senate have held hearings on the vulnerability of Federal information technology to computer crime. These will be discussed in more detail in ch. 5.

[26] See Jim Dray and Fred Wood, OTA, Statement for the Record Before the House Government Operations Subcommittee on Legislation and National Security Hearing on H.R. 2889: The Computer Security Research and Training Act of 1985, Sept. 18, 1985.

[27] See, for example, GAO and other audit reports referenced above; also John O'Mara, "Computer Security: A Management Blindspot," *Computer Security Handbook* (Northborough, MA: Computer Security Institute, 1984), pp. 2A1-2A4; Joel Zimmerman, "The Human Side of Computer Security," *Computer Security Journal*, summer 1984, pp. 7-19.

These factors are most applicable to civilian agencies (and, in many cases, to the private sector as well). In sensitive defense or national security applications where the threats are more apparent (e.g., foreign adversaries), awareness and willingness to spend money for security are likely to be much higher. And, as noted earlier in the chapter, the defense and intelligence agencies have a great deal of expertise in security, and particularly detailed guidance for their staff on appropriate measures for protecting information systems. However, prob-

Competition for Resources

Security measures frequently cost money, and they almost always exact a "tax" on the productivity of information systems. Audit trails that record the activities on a system, for example, require computer time and resources, and they take time and expertise to review. If passwords are required to be more than six characters and changed every 3 months, they are often harder to remember.[28] The use of encryption systems requires time to encrypt and decrypt, time and staff to manage the encoding keys, etc. If given a choice between spending resources on security measures, or spending those resources on features or staff to enhance the performance of an information system, most managers would choose the latter, especially in a climate of tight budgets.

Further, security expenditures are hard to identify and review because security has not usually been included as a separate line item in agency budgets or procurements, and the number of staff hired to handle information security exclusively is usually very small and of relatively low status within the agency. Table 4-10 shows the funding and number of full-time equivalent staff that agencies reported to OTA for computer and communications security. The reported figures are extraordinarily varied, and they probably do not include the full range of information security activities, since (as GAO noted in its study of 25 key systems) agencies tend to be unprepared to account for security costs, and many staff handle information security part-time. However, the total dollar figure reported by all agencies responding ($33.5 million in fiscal year 1985) would seem low compared to OMB's estimate that the government spent $13.9 billion for information technology in fiscal year 1985. Clearly, though, more authoritative numbers than these brief responses to OTA's Federal Agency Data Request are needed as a base for policy action.

OMB's rationale for not segregating security expenditures in budget requests is that security is primarily a component of good information systems management. "It would be a mistake to divide out computer security from computer management. They should be intertwined."[29] Computer systems designers agree that the most productive way to seek out security in information systems is to incorporate security concerns throughout the system's design, implementation, and management. But the net result of OMB's policy might be that, in some cases, system designers do not build in security because they believe it will compete with the funds available for hardware and software that increase performance. As an OMB official noted:

> I would also say that the annual budget process—and I depart a little bit, if I may, from my position as Deputy Director of Office of Management and Budget—tends to emphasize reduced funds rather than increasing expenditures for enhanced telecommunication and data processing and security.[30]

The implementation of NSDD 145 is likely to change the way agencies budget for information security, although the exact nature of those changes has not yet been determined. The directive provides that the Director of NSA shall:

- review and assess annually the *telecommunications* system security programs and budgets of the departments and agencies of the government, and recommend alter-

---

lems in awareness, willingness to spend funds, and clarity of guidance are also significant for some defense applications, particularly those that deal with unclassified information. (OTA, personal communications with Defense Logistics Agency staff, Jan. 22, 1985).

[28] Computer security experts would argue that a well-designed, secure system—one for which security has been designed in from the start and not added later—can run just as efficiently as an insecure one, and in some cases better. In addition, NSA has had some success in using longer passwords composed of real words, such as "ma pa sam," which are more secure than a short password but not as hard to remember as a series of unrelated characters, such as "1xgh7ytrb." (Sheila Brand, National Computer Security Center, personal communication, September 1985).

[29] Joseph Wright, Deputy Director, Office of Management and Budget, testimony to the House Science and Technology Subcommittee on Transportation, Aviation, and Materials hearings on "Computer and Communications Security and Privacy," Sept. 24, 1984, p. 5.

[30] Ibid., p. 4.

Table 4-10.—Federal Agency Expenditures and Staffing for Computer and Communications Security

Agency	Funding (in thousands)			Number FTE[a]		
	1980	1983	1985	1980	1983	1985
Department of Agriculture	$2,295	$ 5,516	$11,866	6.4	17.6	33.0
Department of Commerce	2,565	2,601	2,649	21.0	21.5	22.0
Department of Defense	762	2,900	6,257	35.0	82.5	133.5
Department of Education	0	280	330	—	5.0	5.75
Department of Energy	0	263	170	1.0	0.5	0.5
Department of Health and Human Services	521	486	473	10.25	10.25	13.0
Department of Housing and Urban Development	0	90,000	0	1.0	1.0	1.0
Department of the Interior	132	249	297	2.0	8.0	9.5
Department of Justice	80	234	287	2.0	113.4	134.0
Department of Labor	40	80	120	1.0	2.0	3.75
Department of State	0	520	598	1.0	5.0	8.0
Department of Transportation	46	96	932	10.3	11.3	13.5
Department of the Treasury	164	527	1,607	48.8	14.6	29.4
Subtotal, cabinet agencies	$6,605	$13,842	$25,585	140.0	293.0	407.0
20 selected independent agencies (total)	749	2,362	7,927	62.0	64.0	72.0
Total	$7,354	$16,204	$33,511	202.0	357.0	479.0

[a] FTE = Full-time equivalent staff members.
NOTE: Some figures are rounded.

SOURCE: OTA Federal Agency Data Request.

natives, where appropriate, for the executive agent and the steering group; and

- review annually the aggregated *automated information systems* security program and budget recommendations of the departments and agencies of the U.S. Government for the executive agent and the steering group.[31]

It is not yet clear what kind of authority NSDD 145 confers on NSA and the steering group. One key NSA official said in congressional testimony that while agencies retained autonomy on *whether* to implement security measures, NSA would control *what* would be implemented:

> Once a department or agency head has chosen to spend money on telecommunications security or automated information systems security, the NSA, as National Manager, prescribes or approves which COMSEC [communications security] or COMPUSEC [computer security] technique, system or equipment will be used.[32]

Finding 4 will discuss NSDD 145 in more detail.

Lack of Awareness and Motivation

Another common theme in many of the audit reports cited above is that frequently top agency staff and many general users are unaware of the need for information security. Thus, security staff commonly report that, for example, computer users will write down their password on the wall next to their terminal.[33] This lack of awareness is particularly acute among microcomputer users, most of whom are new to the special security problems raised by the use of their machines. Some of the factors that increase the awareness of computer users toward security needs include press attention, top-level management support, and education and training programs. A later section of this chapter will discuss these in more detail.

Lack of Clear Guidance

Even when agencies are aware of security risks, it is often unclear what measures are appropriate. In short, the current policy guidelines are not clear and specific enough to give Federal managers a concrete idea of what they should do to implement the policies. Circulars A-71 and A-130 do not provide guidance on security measures appropriate for different applications; rather they mandate a risk analysis to help make this assessment. However, agencies have reported increasing frustration with risk analyses. They have frequently been complex, expensive, and oriented toward physical or technical security measures for large-scale computing centers, at the expense of simpler, cheaper, common-sense strategies.[34]

---

[31] Sections 7j-k of the directive (emphasis added). See table 4-4 for the composition of the Systems Security Steering Group.

[32] Walter G. Deeley, (former) Deputy Director, Communications Security, NSA, statement to House Science and Technology Subcommittee on Transportation, Aviation, and Materials, June 27, 1985.

[33] See, e.g., Zimmerman, op. cit.

Federal Government policy and security experts have responded to this problem in several ways. First, substantial efforts are under way to make risk analysis techniques simpler, cheaper, and more helpful.[35] Second, there has been some substantial movement toward developing a set of minimum security standards for various information system applications. Such standards represent a promising technique because they make appropriate actions clear, and eliminate the need for formal risk analyses except in unusual or particularly sensitive situations. As noted earlier, USGS, for example, has reported success in using a technique based on a simple questionnaire that asks system managers to determine the degree of sensitivity of their applications, and to indicate whether they have implemented a set of minimum security measures.

The National Computer Security Center (NCSC)[36] and the NTISSC (the implementing committee for NSDD 145) are also working on a variety of schemes to categorize the sensitivity of unclassified national security-related information and, ultimately, to specify appropriate security measures for each level of sensitivity. In related work, the NCSC has already developed a scheme for categorizing the technical security features of computer systems, ranging from those that require little more than password control (the "C1" level) to those whose operating systems can pass sophisticated tests of design integrity (the "A1" level). The center has an ongoing program for evaluating products submitted by vendors in order to rank them according to their technical security-related features.[37] Each of these categorization schemes is potentially a very important step in helping to make the choice of information security measures for Federal systems clear and explicit.

Finding 4

As NSDD 145 is implemented, it becomes increasingly clear that NSA and the committees guiding implementation of the directive will play a significant if not dominant role in all aspects of information security in the Federal Government whether or not the information is classified. NSDD 145 is likely to result in stronger governmentwide leadership in information security policy; however, concerns have been expressed that it puts the national security community in an unusual, influential if not controlling position on a key aspect of the Nation's information policy.

While the language of NSDD 145 focuses on national security-sensitive information and hostile threats, it also states that NSA is to act as the government's focal point for information security, and

> . . . review and approve *all* [presumably national security-related] standards, techniques, systems and equipments for telecommunications and automated equipment security.

The implementation of NSDD 145 is still in progress, and NTISSC is in the midst of defining sensitive national security-related information and thus the scope of their jurisdiction. However, early indications from participants on NTISSC, as well as congressional testimony by NSA officials, are that the committee may intend to construe their jurisdiction very broadly, to include, for example, information that is sensitive for reasons of privacy, commercial competition, or agency decision-making.[38]

---

[34] See, for example, Robert Campbell, "Agency Risk Analysis Still Inadequate," Mar. 29, 1985, p. 23; and "OMB Directive Is Dramatically Out-of-Date," *Government Computer News*, May 10, 1985, p. 31.

[35] See, for example, the proceedings from the Air Force's first conference on risk analysis techniques, Jan. 21-23, 1985, Montgomery, AL.

[36] The DOD Computer Security Center (under the auspices of NSA) changed its name to the National Computer Security Center in fall 1985.

[37] Department of Defense Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria*, CSC-STD-001-83, August 1983. This is also known as "The Orange Book."

The only other significant technical resource in the government for information security is the NBS Institute for Computer Sciences and Technology (ICST). ICST has approximately nine full-time equivalent staff devoted to information security in the government as a whole (including some working on defense-related security). The National Computer Security Center has more than 200.[39] Thus the de facto assumption behind NSDD 145 is that NCSC can effectively serve as a standards-setter and technical resource for all (or almost all) Federal agency needs for security.

This approach is controversial, with major advantages and disadvantages. Earlier findings in this chapter have documented the need for clear and useful policy action in information security, and the mechanism set forth in NSDD 145 could provide the leadership and visibility to facilitate that action. NCSC can build on a great wealth of expertise in information security matters. In addition, NTISSC provides a significant opportunity for civilian agencies to help guide the process, and it provides an important forum for agencies to share security problems and solutions with each other.

Yet, the same centralization of authority that facilitates leadership and effective action also places NSA (as national manager for computer security) and the Secretary of Defense (as executive agent) in an unusual controlling position on security policy for both military and civilian agencies. This situation has led to heated debate in a 1985 congressional hearing. Representative Jack Brooks, for example, called the directive:

> . . . one of the most ill-advised and potentially troublesome directives ever issued by a President. . . .
>
> First, it was drafted in a manner which usurps Congress's role in setting national policy. . . .
>
> Second, the directive is in conflict with existing statutes which assign to the Office of Management and Budget, the Department of Commerce, and the General Services Administration the sole responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security. . . .
>
> Finally, I seriously question the wisdom of the President's decision to give DOD the power to classify, hence control, information located in the civilian agencies and even the private sector which, in DOD's opinion, may affect national security.[40]

In addition, the extent to which the needs of the civilian side of the government and the private sector mesh well with the needs of the national security sector is open to serious question. Some have asserted that these needs are quite different. For example, before the founding of the Computer Security Center in 1982 some experts argued that the government's primary resource on information security issues should be independent of DOD and NSA.[41] Many of the original arguments against centering the technical resources at NSA concerned the possibility of excessive secrecy. Another disadvantage has recently been argued; namely, that there are important differences between the needs of the national security sector on the one hand, and of the other agencies and the private sector on the other. This disagreement has simmered for several years. In 1984, the *Computer Security Journal* published a "dialogue" between the director of NSA and a prominent private sector computer security consultant. As the journal's editors summarized:

---

[38] A NSA/NTISSC staff member indicated in early 1986 that the NTISSC was leaning toward a definition of "sensitive for national security reasons" that would leave the final judgments in the hands of the agency holding that information. NTISSC would provide criteria to help agencies make such a judgment. This proposal is still in draft form, however.

[39] OTA's interviews with Robert Brotzman, National Computer Security Center, December 1984, and Dennis Branstad/Stuart Katzke, NBS, February 1985. It should also be noted that for several years in a row, the Administration has proposed to eliminate or severely cut the budget of the Institute for Computer Sciences and Technology, which runs the information security and Federal Information Processing Standards programs at NBS.

[40] Representative Jack Brooks, statement before the Subcommittee on Transportation, Aviation, and Materials, House Committee on Science and Technology, June 27, 1985.

[41] Willis Ware, Rand Corp., personal communication, February 1985.

> The DOD position is clearly stated: prevention of unauthorized access is the primary need. Others in the private sector, however, contend that far greater attention must be paid to the potential for system misuse by persons who already possess authorization.
>
> Unfortunately, this difference of outlook is more than an academic disagreement of two parties with fundamentally different needs. NSA has begun actively promoting the idea that its primary need for multilevel access security (unquestionably a real need for national security areas) is shared to a large extent by the private sector. NSA does this openly, with the objective of lowering its own costs by creating a sufficiently large market base to bring about economies of scale. There is a significant concern that this will divert resources away from the real problems of most private sector organizations—and, indeed, of most government agencies as well.[42]

Some observers have noted that the Computer Security Center's position emphasizing outside penetration may be changing, and that it may change further as NSDD 145 is implemented.[43] However, serious differences remain between national security and civilian needs. These tend to occur especially in the marginal zones of security, e.g., applications that process unclassified sensitive data, but do not need and cannot afford NSA-style security measures. Although the NCSC staff say they intend to change and develop more expertise in simpler, cheaper measures[44] the extent to which they will be successful in bridging the traditional gap between their techniques and those outside of the national security community remains to be seen.

Another difficulty with the new NSDD 145 arrangement for some civilian agencies is the secrecy of the procedures involved. Though in fact many of NCSC's activities are open in a way unusual for NSA,[45] NTISSC and related committees guiding the implementation of NSDD 145 require top secret and "SI/TK" special clearances. This prevents many stakeholders from knowing about or influencing the implementation of NSDD 145, and was one of the reasons cited for the previous directive, PD-24, not being as successful as intended.[46] Clearance procedures have also prevented at least one set of civilian agency representatives to one of the NTISSC subcommittees from participating in the first few months of activity because the required clearances had not been obtained.[47] And despite the fact that NTISSC aims to have a broad representation from civilian agencies, several of the largest agencies are not participants, including the Departments of Health and Human Services, Housing and Urban Development, and the Interior. Presumably these agencies were excluded because they have little national security-related data, although they do have data that are sensitive for privacy, agency operations, or proprietary reasons.

The new role of NSA as a result of NSDD 145 is a sensitive subject for other reasons as well. Because of the dominance of the national security agencies in the information security arena, it may be difficult for other individuals and organizations (including consultants or other government officials who work closely with NCSC) to frankly and openly present their views on NSDD 145.[48]

Finding 5

Possible actions to improve Federal information systems security include: more intensive congressional oversight, changing budget procedures with information security receiving higher priority and visibility, designating a ci-

---

[42] "Computer Security, the Defense Department, and the Private Sector—A 3-Part Dialogue About Fundamental Objectives and Needs," *Computer Security Journal*, summer 1984, pp. 53-66.

[43] OTA interviews, Dennis Branstad and Stuart Katzke, NBS, February 1985.

[44] Computer Security Center briefing for Federal agencies on the implementation of NSDD 145, Mar. 15, 1985, Institute for Defense Analyses, Alexandria, VA.

[45] See Sherizen, op. cit.

[46] Clearly, there are reasons for specific information security data to be classified, especially when it could lead a potential adversary to weak points in an agency.

[47] OTA interview with GSA staff, March 1985.

[48] Based on discussions with several key consultants and stakeholders.

vilian agency to be responsible for security training and technical support in the nonmilitary sector, and revising and clarifying NSDD 145.

More Intensive Congressional Oversight

Congress has played a very useful role in deliberations on information security policy, as noted in earlier sections of this chapter. Congressional hearings are a key forum in which broad issues regarding computer and telecommunications security can be openly raised. On the other hand, the management of information security in Federal agencies is intimately linked to many other aspects of agency management, and many Federal officials express the fear that Congress will usurp their management prerogatives if it attempts to determine security policies within agencies.

While it would clearly be unwieldy for Congress to attempt to directly manage information security in individual agencies, there is just as clearly a role for congressional oversight and policymaking in this area. Some of the key aspects of this issue that Congress is well-suited to examine include the balance between military and civilian interests in developing security policy, the usefulness of new programs to facilitate good security practices, and the relation of information security to privacy and other civil liberties.

Congressional hearings focused on the increasing importance of information security, such as those held by the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, help Congress become better informed on the topic. In addition, the various oversight committees in both Houses may wish to include information security as a regular component of their agency oversight hearings, particularly during the implementation of major computer-related programs in agencies. Congress could hold hearings on the willingness of information system vendors to build appropriate security measures into their products. One security expert speculated that the visibility of congressional hearings might be the most effective way to motivate vendors to build in such security, just as car manufacturers routinely include safety features such as seatbelts.[49]

Congress could also maintain close congressional oversight of the implementation of NSDD 145. Possible topics for oversight include the roles of the military and civilian agencies concerning protection of sensitive, unclassified information; the scope and degree of control NTISSC and NSA exert; the effectiveness of the new policy in promoting better information security; and the relation of NSDD 145 to OMB's Circular A-130.

Revised Information Security Budget Procedures

The budget procedures could be changed to provide more visibility for computer and telecommunications security in agency budget requests. Agencies usually do not break out their expenditures for information security, making oversight and cross-agency comparisons difficult. Agencies could specify their expenditures for security (both for staff and as components of information system operating expenses) and/or OMB could conduct a special analysis on this topic. The intent of this would be to make oversight of information security easier; a possible drawback is the additional paperwork that it would generate for the agencies or OMB. OMB and/or GAO[50] could first study in more depth the implications of such a change in budgeting procedures. As an alternative, Congress and/or OMB could request and examine the information security budgets that agencies will be submitting to NTISSC, and could examine closely the portions of agencies' annual internal control reports (submitted under the Federal Managers Financial Integrity Act of 1982) that relate to information security.

---

[49] OTA interview with Robert Courtney, Jr., July 1985.

[50] GAO's recent survey of 25 key Federal computer systems noted that agencies tend to be unable to account for security costs, and argued that lack of such accounting can lead to "uncontrolled overprotection, failure to identify inadequate controls, resource conflicts leading to inadequate safeguards, inability to monitor cost-effectiveness of controls, compare costs, monitor plans, etc." (Statement of William S. Franklin, GAO, before the Subcommittee on Transportation, Aviation, and Materials, app. III, Oct. 29, 1985, pp. 14.)

Designate Civilian Agency for Information Security Training

An existing civilian agency could be designated to provide training and support for computer and telecommunications security in the civilian sector of government. Representative Dan Glickman has proposed a bill, entitled the Computer Security Research and Training Act of 1985 (H.R. 2889), which would formally designate NBS as a lead agency to do background research and establish guidelines for agencies' security training. In addition to the formal designation, the legislation could provide additional operating funds for NBS in this area. Such a measure could strengthen the technical resources on information security on the civilian side of government, help ensure that nonmilitary security needs are met, and reduce the likelihood that NCSC will have a monopoly on computer security policy and practices. On the other hand, this could result in some duplication of effort (although not necessarily undesirable) between the civilian and military sectors.

The Administration has argued that H.R. 2889 is unnecessary because NBS already has an implied mandate to conduct information security research through the Brooks Act of 1965. They also point out that NBS and NSA work together well and coordinate their activities in information security. While both of these points are essentially correct, H.R. 2889 would strengthen and clarify the role of NBS in the new security policy framework of NSDD 145.

Of course, funds for NBS's work in information security could be increased without formally changing the status or designation of NBS in this area.

Revise or Clarify NSDD 145

Congress could codify part or all of NSDD 145 into law, clarifying the roles of NSA, GSA, OMB, NBS, and others in the process. Such an effort should include examining the roles of the central agencies in developing information security policy. To some extent, NSDD 145 contradicts congressional mandates giving OMB and GSA authority to set policy regarding information technology. Codification could help establish a proper congressional role in development of information security policy; on the other hand, a congressionally developed and monitored statute may be less flexible than a Presidential directive, and might hinder the effective implementation of NSDD 145.

Congress or the executive branch could rework the structure and intent of NSDD 145. The degree to which it is appropriate to change NSDD 145 is largely dependent on how much Congress objects to placing NSA and DOD in charge of this aspect of national information policy. NSA and DOD have been, and will likely continue to be, very significant players in information security. In fact, NTISSC itself seems to be a very useful device for agencies to coordinate policy and share ideas on information security. However, by codifying NSDD 145 Congress could remove those aspects of NSDD 145 that give NSA and NTISSC approval authority over civilian agencies' budgets and determinations of information sensitivity. In such a codification, Congress could also develop its own definition of sensitive information that would determine in a general sense the kinds of information agencies should protect. Such an action would diffuse some of the authority of NSA and NTISSC, and thus could dilute some of the potential leadership these groups could assert to improve information security. This option implicitly accepts some dilution of effectiveness in return for a lesser degree of military/national security control over information systems security policy.

The version of H.R. 2889 as amended by the House Committee on Government Operations essentially reworks NSDD 145, giving NBS primary authority for computer security research and training programs for systems that are not used for critical military or intelligence applications.[51] The advantage to defining the

---

[51] Specifically, H.R. 2889 limits NBS's authority to those systems that are covered by the Brooks Act or Paperwork Reduction Act. The wording of those acts explicitly excludes juris-

(continued on next page)

NBS role this way is that there is a much cleaner distinction between the roles of NBS and NSA than there is between information "the loss of which could adversely affect the national security interest" and other information. Thus, such a definition could also help to alleviate concerns about placing the national security community in a controlling position over unclassified civilian information policy. On the other hand, this might work against one of the key purposes of NSDD 145, namely, the desire to improve security of information that was not classified but still critical to the national interest.

(continued from previous page)

diction over information technology that: 1) involves intelligence activities; 2) involves cryptologic activities related to national security; 3) involves the direct command and control of military forces; 4) involves equipment which is an integral part of a weapon or weapons system; or 5) is critical to the direct fulfillment of military or intelligence missions, provided that this exclusion shall not include automatic data processing or telecommunications equipment used for routine administrative and business applications such as payroll, finance, logistics, and personnel management (44 U.S.C. 3502).

APPENDIX 4A.—HIGHLIGHTS OF INFORMATION SECURITY POLICIES OF SELECTED AGENCIES

Department of Agriculture: "ADP Security Manual," DM3140-1, July 19, 1984:

- Separates Automatic Data Processing (ADP) facilities into Type I (large, multi-agency, general purpose facilities), Type II (general purpose computers serving multiple users concurrently), and Type III (other data and word processing equipment).
- Designates application systems as sensitive if compromise could result in fraud or illegal gains, failure to produce time-critical data, violation of national defense disclosure requirements, unauthorized disclosure of private or proprietary data, adverse effect on ongoing investigations or agency operations, or adverse effect in life-threatening situations.
- Requires adequate physical security, designated security officers, annual security reviews, security plans, and backup and contingency plans for critical systems. Facility managers may determine the need for software access controls, data and software protection, and audit trails.

Department of the Treasury: "Information Systems Security," Directives Manual chapter TD 81, Section 40, April 2, 1985:

- Information processed, stored, or communicated by information systems will be placed in three basic categories: national security, sensitive, and public information.
- Sensitive information includes delicate, sensitive, regulatory, financial, law enforcement, privacy, life and mission critical, and proprietary information as well as Officially Limited Information.
- Unauthorized disclosure or manipulation of sensitive information could cause damage such as loss of life or personal injury, loss of property through fraud or theft, loss of privacy, impairment of enforcement or regulatory functions, unfair personal or commercial advantages, or damage to businesses' proprietary secrets.

Department of the Treasury: "Electronic Funds and Securities Transfer Policy," Directives Manual chapter TD 81, Section 80, August 16, 1984:

- Requires the use of the Data Encryption Standard to authenticate electronic funds transactions by the Federal Government. All Federal EFT systems shall be in compliance by June 1, 1988.

U.S. Geological Survey: "Management and Use of Small Computer Systems," Handbook 500-16-H, July 1985:

- Requires small computers to be physically secured during nonbusiness hours or when left unattended.
- Requires backup copies of vital data stored in a separate location.
- Requires users and owners to conduct a risk analysis.

Department of Defense: "Security Requirements for Automatic Data Processing Systems," Directive 5200.28, December 18, 1972 (with revisions, April 29, 1978):

- Emphasizes that ADP systems must be designed with security in mind, and acknowledges the difficulty of adding security measures to systems already in place.
- Describes in very brief and general terms principles for ADP security needs for systems with

different levels of classified information and users with varying levels of security clearances.

- Directs the Assistant Secretary of Defense (Comptroller) to develop and update a manual for ADP security, and to establish a central DOD capability to assist and advise defense agencies in ADP security.
- Requires the head of each DOD component to designate an official to review ADP applications and approve their security safeguards.
- Sets broad goals for ADP security—individual accountability, environmental control, system stability, data integrity, system reliability, communication link security, and appropriate handling of classified material.

APPENDIX 4B.—HIGHLIGHTS OF FINDINGS ON INFORMATION VULNERABILITY BY THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

1. There is no standardized concept of "information sensitivity" among the agencies, and government employees generally are unfamiliar with the term . . . . In contrast to the strong formal programs of [national] security education administered by most agencies, employees are not at all trained in identifying unclassified information which must be protected. [Exceptions include some aspects of protecting documents classified "For Official Use Only" or covered by the Privacy Act.]
2. There is minimal awareness of the vulnerabilities of agency telecommunication facilities to interception.
3. The general failure of government employees and managers to appreciate the threat to vulnerable telecommunications is understandable. Much of the information available on suspected threats to government communications derives from intelligence sources and is classified. It is quite possible, however, to educate employees about potential threats without divulging any classified information.
4. Unclassified information is freely communicated over unprotected circuits without regard to sensitivity.
5. Available telecommunications protection resources are underused or are not used at all.
6. Some stereotyped communications patterns compound the vulnerability problems, [such as] regularly scheduled conference calls which link agencies' top management over private circuits . . . and the use of fixed radio frequencies.
7. A reliance on private lines adds to the vulnerability of sensitive telecommunications . . . . The problems facing the would-be interceptor are drastically reduced by the use of leased circuits as opposed to the use of the public network.
8. Communication systems managers are currently unprepared to take on the foregoing problems.
9. Federal law enforcement activities present an entirely different perspective to the general problems of threat and vulnerability . . . . Several law enforcement agencies are seeking equipment solutions to the vulnerability problems they perceive. NTIA notes that these approaches are uncoordinated.

SOURCE: National Telecommunications and Information Administration, "Summary of Findings of Telecommunications and Information Vulnerability Surveys," Mar. 18, 1983.

Chapter 5

Computer Crime

Contents

Page

Summary 85

Introduction 86

Background 87

Major Findings 91
  Finding 1 91
  Finding 2 95
  Finding 3 95
  Finding 4 97

Tables

Table No. Page

5-1. Types of Computer Crime 86
5-2. The 98th Congress: Essential Characteristics of Computer Crime Bills 89
5-3. The 99th Congress: Essential Characteristics of Proposed Legislation 90
5-4. Commonly Reported Computer Crime Schemes in the AICPA's Study 92

Chapter 5

Computer Crime

SUMMARY

This chapter focuses on evaluating the nature and scope of computer crime, and options to consider in designing effective computer crime legislation. Computer crime is defined here simply as a set of crimes in which computerized data or software play a major role. It is largely the intangible (but critically important) nature of computerized information that creates a need for special legislative attention to computer crime.

Since the 1970s, there has been a growing consensus that existing laws covering the variety of crimes that can be committed using a computer (e.g., fraud, theft, embezzlement, invasion of privacy, trespass) either do not cover some computer abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.

Some of this consensus is a result of publicity regarding "hackers" penetrating various computer systems. The hacker issue is frequently blown out of proportion, and although it cannot be ignored, crimes committed by dishonest or disgruntled employees who have authorized access to computers represent a far greater source of risk than outsiders penetrating information systems.

After a decade of examining computer crime, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. The act provides a felony penalty for those who gain unauthorized access to computerized classified information, and a misdemeanor penalty for unauthorized access to the computerized information of financial institutions or the Federal Government. In addition, 45 States have passed computer crime laws.

OTA's major findings in this area are that:

- There is a scarcity of reliable information about the amount of computer crime occurring and the nature and severity of the crimes. The available evidence suggests that significant losses have occurred, though the full extent is unknown.
- Despite the lack of hard information, the vulnerabilities of organizations using computer systems are much greater than in the past, as discussed in chapter 4 on information systems security. Thus a consensus has emerged that a combination of Federal and State laws is appropriate in this area. Actions taken so far have set forth de facto Federal and State roles—namely, that while State laws will play a primary role in most cases, Federal legislation will concentrate on areas of special Federal concern.
- Legislation needs to balance concern about the potential urgency of the situation with other factors—in particular, the responsibilities of vendors, owners, and users for the security of their systems, and the need for keeping computer crime sanctions reasonably consistent with other criminal law and other aspects of U.S. information policy.

There has been substantial interest in further legislative action on computer crime in the 99th Congress. The legislative debate and hearings have identified the following actions that could clarify and/or strengthen the Federal role in monitoring, preventing, and prosecuting computer crime:

- extend the current Federal statute (Computer Fraud Act) to cover interstate crimes affecting private sector companies, while placing some limits on Federal jurisdiction;
- amend the conceptual approach to defining computer crime used in the Computer Fraud Act, for example, by focusing on the type of crime committed and/or the kinds of information unlawfully accessed;

- change or clarify the kinds of computerized information covered by the Computer Fraud Act, e.g., by restricting the portion of the act that outlaws unauthorized disclosure of information from Federal computers to apply only to Privacy Act information;
- extend or clarify the definitions of key terms used in the Computer Fraud Act, such as the definition of authorization;
- enact limited protection to computer crime victims in order to encourage prosecution;
- enact a penalty for computer crime convictions that would include forfeiture of equipment used;
- establish strengthened or new reporting systems for monitoring the nature and scope of computer crime; and
- establish a study commission to address computer crime (and perhaps related) issues.

INTRODUCTION

As noted in chapter 4, there are four major kinds of measures to protect information systems—technical, physical, administrative, and legislative. The first three were emphasized in chapter 4; this chapter will focus on the problem of designing and implementing Federal legislation that pertains to computer crime.

Generally, computer crime is a term used to refer to a loose set of frauds or abuses in which computerized data or software play a major role. The Department of Justice's *Criminal Justice Resource Manual* defines computer-related crime as "any illegal act for which knowledge of computer technology is essential for successful prosecution."[1] Although some would include theft or physical vandalism of the computer itself in the category of computer crime, the focus of this chapter is on acts that involve manipulation (or theft) of the content of computers—data—for criminal purposes. It is largely the intangible (but critically important) nature of computerized information that makes computer crime a different kind of criminal act needing special legislative attention.

As table 5-1 notes, the computer can be used as a tool or instrument in a variety of activities that resemble distinctly different kinds of "conventional" crimes. While some computer crimes, for example, clearly look like embezzlement, others seem more akin to vandalism or the electronic equivalent of "joyriding." This wide variation in the nature of computer crimes is one of the factors that makes effective, comprehensive, and equitable legislation difficult to design.

Another aspect of computer crime that presents a challenge to effective legislation is the strong connections between this area of legislation and other social and administrative implications of information technology. For example:

- *Computer security* is clearly closely related, in the sense that computer crime laws are part of the arsenal of security measures, hopefully discouraging com-

Table 5-1.—Types of Computer Crime

End result of the crime	"Conventional" crime it resembles
Use of computers to embezzle funds or assets	Embezzlement
Destruction or alteration of software or data	Vandalism or fraud
Unauthorized access to and/or theft of software or data	Theft or trespass
Unauthorized use of computers and computer services	Petty theft, embezzlement, or joyriding

SOURCES: Office of Technology Assessment, and American Bar Association, "Report on Computer Crime," 1984.

---

[1] National Criminal Justice Information and Statistics Service (now Bureau of Justice Statistics), U.S. Department of Justice, *Computer Crime: Criminal Justice Resource Manual*, 1979. (The report was produced by SRI International under contract.) The terms "computer-related crime" and "computer crime" will be used interchangeably in this chapter for the sake of simplicity and adherence to current usage. Computer-related crime is, in a strict sense, more accurate, since in many cases the computer is not the central focus of crime, but rather a tool or a peripheral aspect. (Some would prefer the term "information crime," since the important aspect of the act is not the effect on the machine, but the effect on the information it stores and manipulates.)

puter abuse as well as providing a recourse of last resort for those crimes that do occur.
- *Privacy* is related to computer crime in that such crimes may involve unauthorized access to personal information.
- *Intellectual property* issues are related to computer crime insofar as computerized piracy of software, for example, is a subset of computer crime more generally.[2]

The pivotal nature of computer crime makes it important to recognize these connections in the legislative process to ensure that Federal policies in these areas work in concert.

BACKGROUND

The prime motivating factor for computer crime laws has been the increasingly widespread perception that current laws covering the variety of crimes that computer abuse resembles (e.g., fraud, theft, embezzlement, and trespass) either do not cover some abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.[3]

It is important to distinguish at the outset between computer crimes committed by outsiders who penetrate a system through communication lines (commonly known as "hackers"[4]) and crimes committed by insiders who are authorized to use the computer. The hacker problem has aroused a great deal of media attention, and some of the motivation to finally take action on computer crime legislation seems to be rooted in this phenomenon. The Nation has at times been alternately amused and terrified by reports of teenaged computer hobbyists entering computer systems at Los Alamos National Laboratory, Memorial Sloan-Kettering Cancer Center, and many others. OTA's analysis has led to the following observations:

- There are important differences between hackers who are young experimenters and hobbyists and those who are well-financed, sometimes malicious criminals. There is no question that the significance of teenaged hackers has been overblown. Close examination of many of the incidents tends to reveal that little actual damage was done,[5] or that simple safeguards (e.g., better password control, or dial-back modems) could have prevented the incident. This leaves at least some responsibility in the hands of the system owners who chose not to take "due care" in using such safeguards.

---

[2] A related Office of Technology Assessment study, "Intellectual Property Rights in an Age of Electronics and Information" (forthcoming in 1986), is examining these and related issues in detail.

[3] See, for example, House Judiciary Subcommittee on Crime hearings on Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Sept. 29, 1983, Nov. 10, 1983, and Mar. 28, 1984; Raymond Natter, Congressional Research Service, "Federal Criminal Jurisdiction Under S. 240, 96th Congress: The Computer Crime Bill," Mar. 5, 1979; Nancy Finn and Peter Finn, "Don't Rely On the Law To Stop Computer Crime," *Computerworld*, Dec. 17, 1984.

[4] This chapter uses a working definition of hackers as outsiders who penetrate a computer system they are not authorized to use through communications lines. The etymology of the term is somewhat controversial. Different writers use the term "hacker" to refer to a skilled computer programmer, a computer addict who knows the computer intimately but cannot communicate well with people, or a gifted but sloppy programmer.

[5] Many incidents of computer hacking have resulted in reports of many thousands of dollars in damages, and some incidents doubtless have caused delays and damage. The quantitative estimates of damage are difficult to evaluate, however, because they may include, for example, the costs of damaging publicity about the incident (which are somewhat speculative), or the costs of installing system security measures to prevent an incident from recurring (which are not "damages" but preventive measures that arguably should have been taken before the original incident occurred).

- Nevertheless, there is a growing segment of hacking that is more serious. Some of the reports of crimes committed by hackers seem to indicate a growing level of harm, and there are some reports of increasing involvement of organized crime in hacking, for example.[6] Thus hacking cannot be ignored as a component of the computer crime problem.
- However, as discussed in the previous chapter, computer and security experts are nearly unanimous in their view that the significance of outside penetration into computer systems pales in comparison with abuses by insiders who are authorized to use the computer. Like other kinds of white-collar crime, many of these incidents probably are not reported to law enforcement authorities. External threats may grow in severity, however, as computers are more and more frequently linked by telecommunications systems.

Thus, in designing effective legislation, it is essential to keep in mind the "insider" crimes that have recently received considerably less public attention than have hackers.

Legislative interest. The 94th Congress was the first to consider the subject of computer crime.[7] In addition to several celebrated frauds affecting the private sector in the early 1970s, a 1976 report of the General Accounting Office identified 69 instances of computer-related crimes affecting Federal programs, with resulting losses of over $2 million.[8]

Senator Abraham Ribicoff, Chairman of the Senate Committee on Government Operations (now Governmental Affairs), first introduced the "Federal Computer Systems Protection Act of 1977" in the 95th Congress, and then sent a modified version of the so-called "Ribicoff bill" to the 96th Congress. The bill defined crimes related to:

- the introduction of fraudulent records or data into a computer system;
- the unauthorized use of computer-related facilities;
- the alteration or destruction of information or records; and
- the stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.[9]

Neither the 95th nor the 96th Congresses took final action on this proposal; one of the chief barriers was a concern that the bill expanded Federal jurisdiction too broadly. Since these groundbreaking efforts in this area, both the Congress and State legislatures have considered a myriad of bills, many of them patterned after Ribicoff's original effort. As of late 1985, 45 States have some kind of computer crime legislation.[10] Representative Bill Nelson, after helping to pass an innovative computer crime bill in the Florida State legislature in 1978, introduced a modified version of the Ribicoff bill in the 97th Congress (H.R. 3970, The Federal Computer Systems Protection Act of 1981).[11]

---

[6] Donn B. Parker and John F. Maxfield, "The Nature and Extent of Electronic Computer Intrusion," paper prepared for National Science Foundation Workshop on "Protection of Computer Systems and Software," Oct. 19, 1984.

[7] See, for example, Senate Committee on Government Operations, *Problems Associated With Computer Technology in Federal Programs and Private Industry: Computer Abuses*, June 1976.

[8] U.S. General Accounting Office, "Computer-Related Crimes in Federal Programs," Apr. 27, 1976, FGMSD-76-27. The most famous computer-related crime of the early 1970s was the "Equity Funding" scandal of 1973. Although the fraud did not involve any sophisticated manipulations of a computer, a computer system was used to generate $2.1 billion in fictitious policies. The fraud was based on a pyramid scheme, in which funds from new investors were used to pay off old ones.

[9] Louise Becker, *Computer Abuse and Misuse*, Institute for Defense Analyses, December 1984, p. 29. This document also summarizes the legislative history.

[10] Jay Bloombecker, National Center for Computer Crime Data, Los Angeles, CA, personal communication, February 1986. The five States Bloombecker reports that do not have computer crime laws are New York, Vermont, West Virginia, Indiana, and Arkansas. The District of Columbia's computer crime law is also still under consideration. Bloombecker also reports that three States (Massachusetts, Maine, and Ohio) that are included in the total of 45 made only a minor modification to their criminal code to include data or computer services in the definition of property or services that can be the subject of theft.

[11] The innovative aspect of Florida's computer crime bill is that it defines two new classes of offenses: an offense against intellectual property, and an offense against the authorized computer user. (Finn and Finn, op. cit.)

As interest intensified (in part because of media reports concerning hackers), the 98th Congress considered at least 10 different legislative measures related to computer crime. (See table 5-2 for the titles and essential aspects of the bills proposed in the 98th Congress.)

Ultimately, under the leadership of Representative William Hughes, Chairman of the House Committee on the Judiciary, Subcommittee on Crime, and sponsor of H.R. 5616, the 98th Congress in its final hours passed an amended version of H.R. 5616 as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. (This will be referred to in this chapter as the Computer Fraud Act.) In drafting the bill, Representative Hughes focused on "trespass"—i.e., unauthorized access to specific kinds of information, rather than focusing on the "mere use" of the computer to commit an offense.[12] Thus, the bill provides a felony penalty for unauthorized access to classified information, and a misdemeanor penalty for unauthorized access to the computerized information of financial institutions or the Federal Government. Two further sections of H.R. 5616 that covered any conduct that "affects interstate or foreign commerce" were deleted in final negotiations with the Sen-

Table 5-2.—The 98th Congress: Essential Characteristics of Computer Crime Bills

Bill	Action in 98th Congress	Jurisdiction	Important features
Counterfeit Access and Computer Fraud and Abuse Act of 1984. Public Law 98-473 (H.R 5616, Rep. Hughes)	Passed in continuing resolution, hearings held by House Judiciary Subcommittee on Crime, 9/29/83, 11/10/83, 3/28/84	1) Classified information 2) Federal information systems 3) Financial institution information (deleted sections covering systems affecting interstate commerce)	Oriented toward "trespass," i.e., improper access to the kinds of information defined at left. Gives Secret Service joint investigative authority
Federal Computer Systems Protection Act of 1984 (introduced for the Administration by Sen. Thurmond, S. 2940)	Referred to Senate Judiciary	1) Government computer systems 2) Financial institution computers 3) Crimes involving two or more computers in different States (or countries)	Oriented toward using computer for fraud, damage to systems, unauthorized access. Includes forfeiture of interest in equipment used to perpetrate crime
Federal Computer Systems Protection Act of 1983 (H.R. 1092, Rep. Nelson/S. 1733, Sen. Trible)	Subject of hearing by House Judiciary Subcommittee on Civil & Constitutional Rights 11/18/83	1) Government computer systems 2) Financial institution computers 3) Computers used in interstate commerce	Oriented toward using computer for fraud, and damage to system or data. Derived from Ribicoff bill. Allows State jurisdiction to supersede Federal
Computer Crime Prevention Act of 1984 (S. 2270, Sen. Cohen)	Referred to Senate Judiciary	1) Government computers 2) Financial institution computers 3) Computers used in interstate commerce	Oriented toward fraud, damage, unauthorized use. Same State role as H.R. 1092
Medical Records Protection Act of 1984 (H.R. 4954, Rep. Wyden)	Hearings by House Energy & Commerce, House Judiciary Subcommitteee on Civil & Constitutional Rights, 4/6/84, 8/9/84	1) Medical records	Unauthorized access—misdemeanor; unauthorized access and tampering—felony
H.R. 4384 (Rep. Mica)	Hearings by House Judiciary, Subcommittee on Civil & Constitutional Rights 11/18/83	1) Government computer systems 2) Financial institution computers 3) Computers used in interstate' commerce	Incorporated H.R. 1092 but also sets up computer security research and interagency committee on computer crime
H.R. 4301 (Rep. Coughlin)	Hearings by House Judiciary Subcommittee on Civil & Constitutional Rights 11/18/83	1) Interstate or foreign commerce	3-paragraph bill with harsh penalties for abuse
Small Business Computer Security and Education Act of 1984, Public Law 98-362 (H.R. 3075, Rep. Wyden; S. 1920, Sen. Tsongas)	Passed, hearings by House Judiciary Subcommittee on Anti-trust, 7/14/83, Senate Small Business, 3/7/84	1) Small business	Provides information to small businesses to protect them from computer abuse. Establishes council to advise SBA on computer crimes
Amendment 7101 (Senators Leahy, Mathias, Kennedy, Baker)	Passed by Senate Oct. 11, 1984; dropped in conference	1) Privacy data (restricting Hughes bill jurisdiction over Federal information)	See text for discussion

SOURCES: Office of Technology Assessment, using bill texts and hearing reports, and L. Becker, *Computer Fraud and Abuse*, December 1984.

House Report 98-894 to accompany H.R. 5616, July 24, 1984, p. 20.

ate. One clause would have provided a felony penalty for unauthorized access for the purpose of deliberate fraud resulting in a gain of $5,000 or more within a 1-year period; the other would have provided a misdemeanor penalty for any unauthorized access to computerized information causing a $5,000 gain (for the defendant) or loss (for another) in a 1-year period.

The 98th Congress also passed the Small Business Computer Security and Education Act of 1984, which provides information to small businesses to protect them from computer abuse. While this act does not establish criminal sanctions for computer crimes, its advisory mechanisms could provide further information to help assess the magnitude of the computer crime problem.

In the 99th Congress, there has been substantial interest in further legislative action in this area. Several of the key lawmakers from the debates in the 98th Congress have introduced bills to supplement or change the Computer Fraud Act, as noted in table 5-3, and two other hearings have been held on the topic.[13] The actions proposed in the 99th Congress respond to three major sets of concerns about the Computer Fraud Act:

1. A variety of lawmakers and stakeholders have argued that Federal law should cover interstate private sector computer crimes in some way. H.R. 1001, introduced by Representative Hughes, reintroduces the sections on this topic deleted from the original H.R. 5616. Several of the other measures, H.R. 930 and S. 440, as well as the Administration's bill, H.R. 3381/S. 1678, also expand the law to cover interstate crimes.
2. Some analysts, principally in the civil liberties community, have expressed a concern that the wording of Section 3 of the Computer Fraud Act (specifically the outlawing of unauthorized disclosure of in-

Table 5-3.—The 99th Congress: Essential Characteristics of Proposed Legislation

Bill	Important features	Action in 99th Congress
Counterfeit Access Device and Computer Fraud and Abuse Act of 1985 [amendment] (H.R. 1001, Rep. Hughes)	Revises the act to add conduct "affecting interstate commerce," wording that was deleted from original bill	House Judiciary Subcommittee on Crime held hearings 5/23/85
Computer Systems Protection Act of 1985 (S. 440, Sen. Trible)	Defines jurisdiction to include computers that "operate in, or use a facility of, interstate or foreign commerce." Includes limitation mechanism on Federal jurisdiction, refines definitions	Senate Judiciary Subcommittee on Criminal Law held hearings 10/30/85. Committee also requested comment from Justice and Treasury Departments
National Computer Systems Protection Act of 1985 (H.R. 930, Rep. Nelson)	Similar to above	House Judiciary Subcommittee on Crime held hearings 5/23/85
Medical Records Protection Act of 1984 (H.R. 995, Rep. Wyden)	Affects unauthorized access to medical records through telecommunications device. Provides misdemeanor for access, felony for tampering	Referred to House Energy and Commerce and House Judiciary Committees
S. 610 (Senators Mathias, Leahy, Kennedy, and Cohen)	Amends the act to make unauthorized disclosure of Federal computerized information a crime only if information is covered by the Privacy Act	Referred to Senate Judiciary, Subcommittees on Constitution and on Criminal Law. Committee requested comment from Justice Department
Federal Computer System Protection Act of 1985 (S. 1678, Sen. Thurmond; H.R. 3381, Rep. McCollum)	Administration bill. Outlaws use of computer to commit fraud, contains forfeiture provision for those convicted	Senate Judiciary Subcommittee on Criminal Law held hearings 10/30/85
Computer Pornography and Child Exploitation Prevention Act of 1985 (S. 1305, Sen. Tribie)	Prohibits transmission of lewd or obscene material via computer, especially child pornography	Senate Judiciary Subcommittee on Juvenile Justice held hearings 10/1/85

SOURCE: Office of Technology Assessment. Compiled January 1986

House Judiciary Subcommittee on Crime, Hearing on H.R. 1001 and H.R. 930, May 23, 1985; and Senate Judiciary Subcommittee on Criminal Law, Hearing on Computer Fraud Legislation, Oct. 30, 1985.

formation in Federal Government computers) could be used to restrict informal information flows from government employees to the public or the press. During the 98th Congress, the Senate amended this portion of the bill to restrict its scope so that a person could only be prosecuted for unauthorized disclosure of personal (Privacy Act) information. However, this amendment was not incorporated in the final version of the bill. In the 99th Congress, S. 610 reintroduces this amendment.

3. Some congressional witnesses have argued that the act does not define crimes in a way that is clear and useful for prosecutors, and that the penalties specified—misdemeanors except for crimes involving classified information—are inadequate. (See discussion below.)

In addition, there appears to be substantial congressional interest in the related area of electronic eavesdropping and surveillance, as a result of H.R. 3378 and S. 1667, the Electronic Communications Privacy Act of 1985, introduced by Representative Robert Kastenmeier and Senator Patrick Leahy. The bill would extend legal protections currently applied to voice transmissions to virtually all electronic communications regardless of how they are transmitted. It also makes it a crime to obtain unauthorized access to electronic communications while they are stored in the computer of an electronic communication service, essentially a company providing message-handling services for electronic mail. Thus the bill would make two additions to computer crime law—protecting theft of data while it is being transmitted, and protecting messages in electronic mail systems. However, the bill does not protect stored data that is not associated with an electronic mail or communication system, which is the principal focus of the laws discussed in this chapter.*

As legislative discussion on computer crime has progressed, many key issues and questions have come into focus. In some cases, policymakers and stakeholders seem to be nearing consensus; in others, there are clear differences in approach with which Congress must grapple. The following sections describe some of these areas of agreement and disagreement, and discuss opportunities for further action.

---

*For further discussion relevant to H.R. 3378 and S. 1667, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985).

MAJOR FINDINGS

Finding 1

There is a scarcity of reliable information about the amount of computer crime occurring and the nature and severity of the crimes. The available evidence suggests significant losses, though the full extent is unknown.

Recently, considerable attention has been focused on computer crime, particularly the small component of such activity that is committed by teenaged hackers.[14] Beyond anecdotes provided by the media, a number of organizations have attempted to develop evidence about the nature and scope of computer crime. Some of the highlights of these studies are reported below, with the caveats that each was limited in scope, was the first study of its kind, and had significant methodological flaws. Thus, the data and descriptions provided below represent only an impressionistic sketch of the computer crime situation, not an authoritative picture. The policy discussion at the end of this chapter will discuss needs for further information about computer crime.

The *American Bar Association (ABA)*[15] surveyed public and private sector organizations for their views on and experiences with computer crime.[16] Twenty-five percent (72) of the respondents reported "known and verifiable losses due to computer crime during the last 12 months." Fifty-four of the respondents reported that their total annual losses due to computer crime were between $0 and $100,000, while four respondents were in the $10 million to $50 million range, and one reported losses between $100 million and $500 million. The larger figures are staggering and, because the study was anonymous, cannot be substantiated. ABA notes that these figures cannot be extrapolated to the Nation as a whole and comments that many estimates of economic losses attributed to computer crime are "unexplained" and "unsupported."

---

[14] For examples of such attention, note *Newsweek* coverage of computer crime (Sept. 5, 1983, pp. 42-48; and Aug. 29, 1983, pp. 45-49); and the movie "War Games."

[15] "Report on Computer Crime," Task Force on Computer Crime, Section on Criminal Justice, 1984. Also see analysis in Louise Becker, *Computer Fraud and Abuse*, Institute for Defense Analyses, December 1984.

The *American Institute of Certified Public Accountants*[17] conducted a survey of 5,127 banks and 1,232 insurance companies. Two percent (105) of the banks and 3 percent (40) of the insurance companies said they had experienced at least one case of fraud related to electronic data processing (EDP), a dramatically lower proportion of crime incidence than the ABA study although the methodology for the two studies is quite different. The study was not intended to provide reliable data on the incidence or the magnitude of frauds in insurance or banking, but rather to analyze the "general nature and means of committing some EDP-related frauds." Table 5-4 indicates some of the schemes reported for these frauds, from most to least frequent. The most frequent perpetrators of these frauds were clerical personnel (for smaller frauds) and mid-level management or supervisory personnel (for larger frauds). Only 16 percent of the frauds were reported to involve more than $100,000, and that figure does not reflect any funds recovered.

Table 5-4.—Commonly Reported Computer Crime Schemes in the AICPA's Study (from most to least frequent)

Banking	Insurance
• Divert customer funds into perpetrator's own account • Make unauthorized extensions of credit limits, loan due dates • Create fictitious loans • Defer recording of perpetrator's own checks and charges • Forge customer input documents (checks and withdrawals) • Make ATM extractions • Make adjustments to customer deposits • Divert loan payments into perpetrator's own account • Divert customer income to perpetrator's own account • Wire transfer	• Create fictitious claims • Trigger unauthorized refund or reduction of premiums • Create unauthorized policy loans • Trigger unauthorized dividend withdrawals • Forge checks • Create unauthorized mortgage loans • Reinstate lapsed policies • Create fictitious pension payments

SOURCE: American Institute of Certified Public Accountants, EDP Fraud Review Task Force, "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," 1984.

In 1983, the *President's Council on Integrity and Efficiency* released a report on the first phase of a study on computer-related fraud and abuse. The panel surveyed Federal agencies and found a total of 172 relevant cases (69 fraud, 103 abuse). The losses in fraud cases ranged from $0 to $177,383, with the highest proportion in the $10,000 to $100,000 range. However, noting that many agencies do not keep reliable or systematic data in this area, the leader of the study told a congressional committee that:

> One overriding finding of this study is that we still do not know the scope of computer-related fraud and abuse in government.[18]

A follow-on study by the Inspector General of the Department of Health and Human Services contained interviews and analyses of 46 perpetrators of computer-related fraud cases in the Federal Government. Although it is not known to what extent these perpetrators are representative, in general they:

---

[16] According to congressional testimony, "The survey was sent to approximately 1,000 private organizations and government agencies, including the Fortune 500 companies, banks, insurance companies, financial services, brokerage firms, accounting firms, all major Federal departments and agencies, all State attorneys general, and a sample of district attorneys." Responses were received from 283 organizations. (Testimony of Joseph B. Tompkins, Jr., to House Subcommittee on Transportation, Aviation and Materials, Sept. 24, 1984).

[17] American Institute of Certified Public Accountants, EDP Fraud Review Task Force, "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," 1984.

[18] Richard P. Kusserow, Inspector General, Department of Health and Human Services, testimony to House Subcommittee on Transportion, Aviation, and Materials, Sept. 24, 1984.

- were insiders, and were typically young, well-regarded employees;
- held a wide variety of positions, although most commonly were caseworkers, clericals, or data-entry technicians;
- typically committed their crime by manipulating input data to cause funds to be issued, and most were aided by co-conspirators;
- committed the criminal activity over a 6-month period, on the average;
- stole in response to a situational stress, such as personal indebtedness; and
- didn't think about the consequences of their actions, or assessed the risks of getting caught as minimal.[19]

The *Department of Justice Bureau of Justice Statistics* (BJS) has commissioned various reports to try to assess the nature and scope of computer crime. One recent BJS report examined the scope of fraud related to electronic funds transfer in a confidential survey of 16 banks. Because of the small sample size, this pilot study's results should be viewed as suggestive only. The study estimated that banks nationwide lost $70 million to $100 million during 1983 from automatic teller fraud. This is only about 0.03 percent of a total volume of $262 billion processed through automatic tellers, or a loss of 32 cents per $1,000 of transaction volume. The study also examined potential losses from wire transfers, although there were insufficient data to estimate national loss levels. Twelve banks reported 139 wire transfer fraud incidents within the preceding 5 years, with an average exposure to loss (before recovery efforts) per incident of $883,279, and an average net loss (after recovery efforts) per incident of $18,861. By comparison, roughly 60 million wire transfers were completed in 1980, involving $117 trillion.[20]

Consultants and other researchers have also played significant roles in assessing the nature and scope of computer crime. In one recent study, two researchers conducted telephone interviews with 106 law enforcement officials and prosecutors in States that had computer crime statutes. Sixty-seven investigations under the new computer crime laws were identified, leading to 56 indictments and 32 convictions. The authors found:

- only a few of the many incidents investigated resulted in prosecution, primarily because the evidence available did not appear to support indictment. Some prosecutors reported that grand juries failed to understand the case because of the technical nature of the acts involved;
- more perpetrators now seem to be mounting a defense than did those prosecuted in the past. The most actively defended recent cases have been those involving electronic trespass;
- many prosecutors interviewed were unaware that their State had a computer crime law;
- some prosecutors reported that because penalties for violation of their computer crime laws are less than those for traditional theft and burglary laws, they favor use of the more stringent statutes; and
- many prosecutors chose to use the computer crime law only when a traditional fraud, theft, or malicious mischief statute was clearly less applicable. Therefore, this report likely covers only a small proportion of all computer crimes because of the preponderance of cases prosecuted under other laws. The most experienced prosecutor of computer crimes in California strongly supports this conclusion.[21]

SRI International has also kept a file of computer crime incidents, principally consisting of media reports. However, SRI's lead investigator in this area has for some time argued forcefully that none of the figures quoted on the subject of computer crime (including

---

[19] Richard P. Kusserow, "Computer-Related Fraud in Government Agencies: Perpetrator Interviews," published by the Department of Health and Human Services, May 1985.

[20] Bureau of Justice Statistics Special Report NCJ-96666, "Electronic Fund Transfer Fraud," March 1985.

[21] Susan Nycum (Gaston Snow & Ely Bartlett), and Donn Parker (SRI International), "Prosecutorial Experience With State Computer Crime Laws," February 1985, pp. 15-16 (unpublished paper).

SRI's) are reliable.[22] This researcher and another veteran of computer crime debates have written:

> No valid statistics representative of the computer crime problem currently exist. Although many estimates have been published and often quoted, investigation has shown that these are not representative, primarily because of the following:
>
> - Few victims are willing to report incidents and suffer the staff-time expense, embarrassment, civil liabilities, business disruption, questionable basis for litigation, and violation of security by revealing vulnerabilities.
> - Definitions of what constitutes a crime differ from state to state so that events cannot be consistently measured.
> - No successful collection mechanisms for statistics have been discovered and developed. . . .
>
> The lack of statistics measuring the size of the problem has been a source of concern. Although news media attention on spectacular individual cases has created the image of a very serious problem, the absence of valid data makes establishing rational legislative priorities and characterizing the problem difficult.[23]

In contrast, another prominent computer security expert argues that it is, in fact, quite possible to develop usable data on computer crime, although he acknowledges that "statistical analyses of data on computer-related crime do not lead to the predictability of such crime in any particular working environment."[24] Of the 1,406 cases tracked by this author as a part of his role as a security consultant, he reports that there is an average loss of $500,000; that 89 percent are never taken to the criminal justice process; and that of the 11 percent that are, convictions are obtained in only 18 percent.[25]

The *Justice Department's Fraud and Corruption Tracking (FACT) System*, begun in 1983 primarily to track cases involving fraud in the Federal Government, reported 8 computer-related crimes out of 3,112 fraud and corruption cases in 1983, and 18 out of 3,582 in 1984. The system includes only cases prosecuted by the FBI and those at agencies that Congress has mandated to be monitored under the FACT System. Most of the cases involved false data entry to get unauthorized benefits from unemployment or welfare programs.[26]

In short, only a few scattered pieces of information are available on computer crime; much of the quantitative information is analytically soft; and in some cases, the studies conflict with one another. Some of these studies, such as the ABA report, seem to suggest fairly widespread patterns of computer crime; some of the others indicate a significant amount of such criminal activity, but with the full extent unknown.

It is arguable how much could reliably be known about the nature and scope of computer crime. Like many other white-collar crimes, companies may not want to report these incidents to law enforcement agencies, particularly in the case of large losses that may result in embarrassment or exposure of vulnerabilities. However, it is possible that more focused study of computer crime could improve the soft information now available. For example, one congressional witness suggested that a large-scale "victimization study," undertaken by professional criminologists, could add substantially to knowledge in this area.[27] This issue will be discussed further at the end of this chapter.

---

[22] Donn Parker, SRI International, OTA work session, Jan. 25, 1985.

[23] Nycum and Parker, op. cit., pp. 2-3.

[24] Robert Courtney, Jr., and Mary Anne Todd, "Problem Definition: An Essential Prerequisite to the Implementation of Security Measures," paper prepared for presentation to The Second International Congress and Exhibition on Computer Security, Toronto, Sept. 10-12, 1984.

[25] Robert Courtney, Jr., Interview with OTA staff, July 17, 1985. Because Courtney does not divulge the details of his cases in order to preserve the anonymity of his clients, his data are not open to other expert scrutiny.

[26] Glenn McLoughlin, Congressional Research Service, Library of Congress, "Computer Security and Crime," Issue Brief IB85155, Oct. 22, 1985.

[27] Sanford Sherizen, testimony to Senate Small Business Committee, Mar. 7, 1984.

Finding 2

Despite the lack of hard information, the vulnerabilities of organizations using computer systems are much greater than in the past. Thus a consensus has emerged that a combination of Federal and State laws is appropriate in this area.

As discussed in chapter 4, rapidly changing technical and social factors have increased the risks and potential losses related to information systems by an order of magnitude. These changes include increased networking, the advent of microcomputers, increased dependence on information systems, and increased computer literacy. The increasing awareness of these new levels of risk, and resulting consensus in support of Federal legislative action, can be seen both in the actions of Congress (passing, without dissent, the Computer Fraud Act), in substantial testimony to Congress, and in the opinions of many experts and groups.[28]

This apparent consensus is a very significant change from earlier sentiment in Congress. In many of the earlier hearings on computer crime, the view was expressed that the existing network of statutes covering, for example, wire and mail fraud, embezzlement, and privacy should be adequate to cover computer crime, and/or that it should primarily be under State jurisdiction.[29]

While some might still debate this point, the Federal and State actions taken so far have, in essence, accepted the need for legislation, and set forth Federal and State roles in this area of crime—namely, that while State laws will play a primary role in most cases, Federal legislation will concentrate on areas of special Federal concern: e.g., Federal records, financial information, classified information, and possibly interstate crimes and medical records.

One potential problem with this de facto allocation of roles in the area of computer crime is that different State laws are frequently inconsistent. One legal expert has suggested that a body such as the National Conference of Commissioners on Uniform State Laws could focus on computer crime laws and possibly draft a uniform model State law.[30]

Finding 3

Legislation needs to balance concern about the potential urgency of the situation with other factors—in particular, the responsibilities of vendors, owners, and users for the security of their systems, and the need for keeping computer crime sanctions reasonably consistent with other criminal law.

Because the nature and value of intangible data are difficult to assess, and because it is often hard to distinguish myth from reality where computers are concerned, it is easy to overreact to stories about computer crime.

For example, computer professionals argue that many computer systems are irresponsibly left unprotected because simple precautions are not taken—the computerized equivalent of leaving piles of money in bank windows. Such simple precautions include, for example, requiring the authority of two persons for disbursements, maintaining logs of system activity and scanning them for unusual patterns, changing standard passwords that are set for every system when they are first turned on, or using "dial-back" modems that require users to be at their authorized terminal locations. (See ch. 4 for further discussion of security measures.) Thus, some would argue that the urgency of the need for computer crime legislation is considerably less than commonly perceived because of these systems that are left irresponsibly unprotected.[31]

---

[28] See, for example, testimony to House Judiciary Subcommittee on Crime, Sept. 29, 1983, Nov. 10, 1983, and Mar. 28, 1984; testimony to the House Science and Technology Subcommittee on Transportation, Aviation, and Materials hearings on Computer and Communications Security and Privacy, Sept. 24, 1984; and testimony to the Senate Governmental Affairs Subcommittee on Oversight of Government Management, "Computer Security in the Federal Government and the Private Sector," Oct. 25-26, 1983. The American Bar Association and American Institute of Certified Public Accountants reports cited previously also argue forcefully for legislative action. In addition, the Data Processing Management Association, Videotex Industry Association, and Information Industry Association have each drafted model computer crime bills and urged Federal computer crime legislation. The Computer and Business Equipment Manufacturer's Association supported Representative Nelson's bill, H.R. 1092. And, a 1983 survey of 637 members of the American Society for Industrial Security indicated that 93 percent of the respondents felt a need for computer crime legislation at the Federal level (presented in Senate hearings, above, p. 163). Also see Finding 1 and discussion in ch. 4.

[29] See, for example, Senate Judiciary Subcommittee on Criminal Justice, "Hearings on S. 240, Computer Systems Protection Act of 1979," Sept. 23, 1982.

[30] Daniel Burk, "The Philosophies of Computer Crime Legislation: An Editorial Collection," *Computer Law Reporter*, vol. 3, No. 3, November 1984.

This is not to say that legislation is not needed. Car theft is illegal, for instance, even though many people leave their car doors unlocked—but it does raise the importance of both the Federal Government and the private sector pursuing computer security at the same time that computer crime law is being developed. That is, legislation alone is not a solution to computer crime. These relationships between computer security and computer crime highlight the need for Congress to coordinate its efforts in examining the two topics.

Further, as noted earlier, the gravity of many of the incidents of computer hacking has been exaggerated. For instance, the system that hackers broke into at Los Alamos National Laboratory in 1984 was new and still undergoing testing.[32] In fact, one participant in OTA's work session on information security, whose views are shared by many in the computer science research community, argued that we should not discourage young people from hacking:

> A lot of the people who are known as pretty good programmers started out as hackers 15 or 20 years ago poking around in systems because that was the only option available. In many respects that was also the best thing we could do for our society, which after all built its mid-century experience on whole generations of people who learned auto mechanics souping up their cars to violate the speed laws.
>
> This poking around used to encourage teenagers to go into computing. And if the lure of a little illicit playing around in somebody else's computer is doing that, the benefits for our society are going to far outweigh the inconvenience of having a few people who weren't careful enough and had their files damaged by inexperienced people playing around on the computers.[33]

This view is quite controversial, although significant as a counterpoint to other voices that argue for strict computer crime laws. It should be interpreted in the spirit in which it was intended—as a warning against excessive penalties for nonmalicious experimentation, not as an argument that criminals who use computer hacking to commit crimes should be sanctioned by the law. And clearly there are some systems in which experimentation is more tolerable than others—at schools of computer science, for example, where hacking is even tacitly encouraged—while there are others that are far more sensitive and should be well protected, both by law and by security measures.

A second important broad concern is the need for keeping standards and practices for computer crime reasonably consistent with standards and practices for other kinds of criminal activity. For example, one scientist compared an employee "stealing" computer time to do personal work (a much discussed form of computer abuse in computer literature and congressional hearings) to a machine tool operator who uses the shop's equipment after hours for personal work. The policy for such activity varies among machine shops from forbidden to encouraged, but it is generally not considered a criminal offense.[34]

Finally, it is worth noting that there are potential disadvantages to being overzealous in computer crime legislation. This is related to a question that Senator Paul Laxalt raised in 1980 hearings:

> By focusing on the computer as an instrumentality, are we exposing individuals to criminal liability for possibly innocent conduct while not furthering the public safety?

Previous OTA testimony also warns against "criminalizing bad manners":

---

[31] OTA work session on information security, Jan. 25, 1985.

[32] Suzanne Smith, Los Alamos National Laboratory, Remarks to Air Force Federal Information Systems Risk Analysis Workshop, Montgomery, AL, Jan. 22, 1985.

[33] OTA work session, Jan. 25, 1985.

[34] The Computer Fraud Act does not criminalize the unauthorized use of computer time for personal purposes, although some State statutes do.

> Not all instances of unethical behavior are illegal. Behavior such as eavesdropping on private conversations and snooping into private papers by individuals is not totally covered by law. Instead, society regulates it through a less formal system of social rewards and punishments. As communications increasingly take electronic form and as laws and regulations are passed, such behavior may become subject to formal criminal rather than informal social sanction. Maybe in many cases it should be treated so, but we may need to build sufficient flexibility into the law to avoid criminalizing all bad manners.[35]

Overly restrictive or intimidating legislation could also, for example, stifle productive flows of information from government to the public, or stifle productive and creative activities on the part of computer users. Several critics of the Computer Fraud Act have argued that the law could be used by agencies bent on secrecy to prosecute employees for informally divulging computer-based information to the public or the press—even if that information was available to the public under the Freedom of Information Act.[36]

Finding 4

A number of possible actions have been identified to clarify and/or strengthen the Federal role in monitoring, preventing, and prosecuting computer crime. Congress has already enacted computer crime legislation,[37] but there are a substantial number of proposals before the 99th Congress to fine-tune or change the Computer Fraud Act in some way (see table 5-3).

Congressional witnesses and others have raised several important doubts about the adequacy of the new act for effective prosecution of violators, based on the limited experience currently available. Two major problems reported by prosecutors are:

1. the fact that the act only provides for misdemeanor penalties unless the information accessed is classified. This may not be sufficient incentive to proceed with a criminal case; and
2. the act's wording, which defines a crime as an unauthorized access that "affects" a government or financial institution computer. Some argue that "affect" is a vague and overly broad term.[38]

The legislative debate and hearings have identified several actions that could strengthen and/or clarify the Federal role in monitoring, preventing, and/or prosecuting computer crime. These are discussed briefly below.

Extend the Federal statute to cover interstate crimes affecting private sector computers.

In part because of considerable variation in State laws governing computer crime (and because a few States still do not have computer crime laws), a Federal statute could clarify and standardize policies for interstate crimes. However, the definition of "interstate" needs to be carefully examined. Several of the computer crime bills cover systems that "affect interstate or foreign commerce,"[39] or "operate in, or use a facility of, interstate commerce."[40] This could cover a very large number of information systems and prospective crimes if Federal officials chose to interpret it that way. Many businesses routinely exchange information between their computers located in several States; almost all systems use a telecommunications carrier that operates across State lines. The Administration bill (S. 1678 in the 99th Congress), on the other hand, covers only crimes in which "two or more computers are used which are located in different States or in a State and a foreign country." The Administration wants a limited Federal role in the area of computer crime, in line with its understanding of Federal/State roles.[41]

---

[35] Testimony of Frederick Weingarten, Program Manager, Communication and Information Technologies Program, Office of Technology Assessment, before the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice, "Electronic Surveillance and Civil Liberties," Oct. 24, 1985.

[36] *New York Times*, "Computer Privacy, Not Secrecy," Oct. 11, 1984; and Allan Adler and Jerry Berman, American Civil Liberties Union (ACLU) Memo on "Need to Revise Newly Enacted Computer Crime Statute," January 1985.

[37] See table 5-2. Both the Counterfeit Access and Computer Fraud and Abuse Act of 1984 (Public Law 98-473) and the Small Business Computer Security and Education Act of 1984 (Public Law 98-362) were enacted in the 98th Congress.

[38] See May 23, 1985, hearing of the House Judiciary Committee, Subcommittee on Crime, on "H.R. 1001 and H.R. 930, Bills relating to Computer Crime and Computer Security"; and Mitch Betts, "U.S. Attorneys Push To Clarify Vague '84 DP Crime Law," *Computerworld*, July 1, 1985.

[39] H.R. 1001 in the 99th Congress, Representative Hughes.

[40] S. 2270 in the 98th Congress, Senator Cohen.

Because of the fluid nature of telecommunication networks, computerized information may cross State lines in transmission even if the perpetrator is in the same State as the host/victim computer. Thus, in general, establishing the site of the computer crime, and hence the jurisdiction, can be difficult. Because of this difficulty, OTA found that it would be useful to have broad wording for the definition of "interstate" in Federal computer crime cases, while at the same time providing a checking mechanism so that Federal jurisdiction does not expand without bounds. Several bills provide for Federal jurisdiction while adding such a mechanism by allowing State jurisdiction to supersede Federal under certain conditions, through a careful weighing of priorities and Federal interest in the case.[42] Another advantage of providing this option for State officials is that they can use the expertise of the FBI or Secret Service if necessary; Federal involvement could also help to standardize State treatment of computer crime cases. To further standardize State approaches to computer crimes, Congress may also wish to commission or participate in the development of a model State computer crime act, as discussed earlier.[43]

Amend the conceptual approach to defining computer crime used in the Computer Fraud Act.

There are at least two basic ways legislation could define computer crimes and address sanctions:

1. laws could declare it a crime to access certain kinds of information or to make unauthorized use of the machine itself essentially a kind of *trespass;* or
2. laws could concentrate on the nature of the crime committed while using a computer, essentially a *tool* approach.

The Computer Fraud Act and Representative Hughes' proposed amendment in the 99th Congress, H.R. 1001, both take the trespass approach because they define crimes according to unauthorized access to particular types of information, or unauthorized use of computers (in H.R. 1001, for interstate computer crime). Most of the other bills take the "tool" approach, focusing on use of the computer to defraud. This approach does not require that prosecutors prove access was unauthorized, which can be difficult for insider crimes.

An interesting variation on the "tool" approach are model computer crime acts drafted by the Videotex Industry Association and Data Processing Management Association in 1984; these model acts define different kinds of crimes such as "computer fraud," "damage or destruction of computer property," "computer trespass," and "theft of computer property or services." The Virginia computer crime act adopts this approach, defining five new crimes: computer fraud, computer trespass, computer invasion of privacy, theft of computer services, and personal trespass by computer.[44] These categories are similar to those outlined earlier in table 5-1.

---

[41] Statement of John C. Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice, to House Judiciary Subcommittee on Civil and Constitutional Rights hearings, Aug. 9, 1984

[42] The Nelson (H.R. 930 in the 99th Congress), Trible (S. 440 in the 99th Congress), and Cohen (S. 2270 in the 98th Congress) bills have this provision. They say that in cases of concurrent Federal and State or local jurisdiction, Federal law enforcement officers should consider the relative gravity of the Federal offense and the State or local offense; the relative interest in Federal investigation or prosecution; the resources available to the Federal authorities and the State or local authorities; the traditional role of the Federal authorities and the State or local authorities with respect to the offense; the interests of federalism; and any other relevant factor. (S. 440, Section 6b.) These bills also provide for periodic reports to Congress on the effect of the law on the scope of Federal jurisdiction. The provisions for balancing State and Federal interests in establishing jurisdiction are already reflected to some extent in internal Department of Justice policies. (Ed O'Connell, House Judiciary Subcommittee on Crime, personal communication, January 1986.)

[43] For good analyses of some of the differences between State laws in this area, see Becker, op. cit., and Nycum and Parker, op. cit.

[44] Virginia Computer Crimes Act, Virginia Code Section 18.2-152.1 et seq., signed by the Governor Apr. 11, 1984. The act also expands the definition of embezzlement in Virginia's criminal code to include embezzlement of computer time and services. For a discussion see Daniel Burk, "Virginia's Response to Computer Abuses: An Act in Five Crimes," *Computer Law Reporter*, July 1984.

Because this kind of "tool" approach connects computer crimes closely to traditional (noncomputer) violations that the computer crimes resemble, it may be easier for many people (and perhaps prosecutors) to understand. However, sentiment in the 99th Congress, as evidenced by the proposed legislation, is either to retain the conceptual framework of the Computer Fraud Act with some additions or modifications, or to adopt a simplified "tool" approach. The Administration's bill essentially uses this latter approach, focusing on fraud or theft committed with the computer.

Change the kinds of information covered in Federal legislation: to include medical records, to clarify the law regarding disclosure of public information, and/or to clarify the definition of "financial institution."

Three possible changes have been clearly identified. One would extend coverage to include medical records. Interest in this measure was aroused by reports of a hacker break-in at Memorial Sloan-Kettering Cancer Center in New York in 1983.[45] However, the relative frequency and seriousness of threats to medical records have not received close study. The Administration argues that tampering with medical records should be considered an issue of State law, unless the records are those of a Federal agency or Federal medical facility.[46]

The second potential change in the kinds of information covered in the Computer Fraud Act is the option of restricting the kinds of information covered in section 3 (Federal records). S. 610 modifies subsection a(3) of the Computer Fraud Act; while it is still a crime to modify, destroy, or use Federal information, the disclosure of information is outlawed only if the information is protected by the Privacy Act. As mentioned earlier, Senators Leahy, Mathias, Kennedy, and Baker,[47] civil liberties advocates,[48] and others argued that making a crime of unauthorized access and disclosure of *any* Federal computerized information would restrict Congress and the public's access to information whose disclosure is not restricted if it were not in a computer. While Representative Hughes has asserted that this should not be a problem since a "whistleblower" or other Federal employee who wanted to pass on information informally would have authorized access to the computer, conceivably the agency involved could argue that the disclosure was a "purpose for which such authorization does not extend." OTA found that restricting the unauthorized disclosure phrasing in this paragraph could help clarify the statute, and deserves careful consideration.

Third, the Department of Justice[49] has testified that the definitions of financial information protected by the 1984 Computer Fraud Act are unwise because they restrict coverage to financial records as defined by the Right to Financial Privacy Act of 1976, or credit agency records as defined in the Fair Credit Reporting Act. Thus, in the Justice Department's interpretation, the act's definition excludes the bank's own records, as well as records on corporations. The Administration bill would cover frauds or thefts perpetrated with access to any financial institution computer.[50]

---

[45] See Representative Wyden's testimony to House Judiciary Civil and Constitutional Rights Subcommittee, Aug. 9, 1984.

[46] John C. Keeney, Deputy Assistant Attorney General, testimony, Subcommittee on Civil and Constitutional Rights, Aug. 9, 1984.

[47] *Congressional Record*, Oct. 11, 1984, pp. S14403, S14445.

[48] See ACLU memo, and *New York Times*, op. cit.

[49] Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, Department of Justice, testimony before the House Judiciary Subcommittee on Crime, Oct. 30, 1985.

[50] A related piece of legislation, the Computer Pornography and Child Exploitation Prevention Act of 1985 would criminalize use of a computer to transmit obscene, lewd, or lascivious writing, descriptions or pictures, or information pertaining to sexual exploitation of children. While preventing exploitation of children is clearly a desirable goal, defining obscenity by computer is no easier than defining it in other media, and keeping standards for "electronic pornography" reasonably consistent with other laws and social standards, such as first amendment rights to free expression, is difficult. A full analysis of this legislation is beyond the scope of this report. (See, for example, Mitch Betts, "Regulation of Bulletin Boards Faces Strong Opposition," *Computerworld*, Sept. 9, 1985; T.R. Reid, "Big Brother Trible Has His Eye on Your Personal Computer," *The Washington Post/Washington Business*, Sept. 16, 1985, p. 5.) For arguments in favor of this legislation, see testimony presented at the Oct. 1, 1985, hearing of the Senate Committee on the Judiciary, Subcommittee on Juvenile Justice.

Establish strengthened or new reporting systems for monitoring computer crime.

The Department of Justice and FBI, for example, could further expand their ability to develop effective statistics on computer crime, or could conduct or sponsor further studies of the topic. Although there have been several efforts to develop information about computer crime, the resulting information is unsatisfactory from the point of view of legislators trying to judge the severity of a problem. There are two aspects to this problem—information about the pervasiveness of computer crime in society and business generally, and specific information about computer crimes within the Federal Government.

Based on the weaknesses of current studies as discussed in Finding 1, OTA found that a further effort to assess the nature and scope of computer crime in society and business generally would be most worthwhile if the effort:

- is large-scale, well-funded, and run by a credible and impartial organization, so that the results will be authoritative;
- includes both quantitative studies of the scope of computer crime and qualitative information on the nature of the crimes, how they are evolving, and what influences organizations in deciding whether to prosecute;
- includes the expertise of professional criminologists who have developed relatively sophisticated techniques for interviewing victims of crime;
- compares computer crimes to other forms of white-collar crime in nature, evolution, and prosecution aspects;
- compares an organization's susceptibility to computer crime to its computer security measures; and
- guarantees the anonymity of the victim organizations contacted.

In addition to such a study of computer crime in general, Congress could direct further studies of such crime within the Federal Government. There are several good beginnings toward collecting such data—e.g., the two reports issued by Richard Kusserow, Inspector General of the Department of Health and Human Services; and the Fraud and Corruption Tracking System at the Department of Justice. However, only 19 percent (25 of 130) of agencies responding to OTA's Federal Agency Data Request reported that they had an established procedure for tracking and analyzing computer crime within their agency. Such procedures could be mandated.

Other actions that have been suggested include:

—Clarifying the definition of "authorization" in the Computer Fraud Act.

This could help make the Computer Fraud Act clearer since this concept underlies the whole statute. A definition proposed as an amendment to the Virginia statute (although not yet taken up by the legislature) could be a useful starting point:

> A person is "without authority" when he has no right or permission of the owner and no reasonable grounds to believe that he has such right or permission, or, he exceeds such right or permission. It shall be an affirmative defense to a prosecution under this act that: 1) the person reasonably believes that the owner, or a person empowered by the owner, has given authority to that person; 2) the person reasonably believes that the owner, or a person empowered by the owner, would have given authority without payment of any consideration; or 3) the person reasonably could not have known that he was without authority.[51]

—Enacting a limited provision to protect competitive secrets of victim organizations during prosecution, in order to encourage prosecution of computer crime.

Since a key reason why companies do not prosecute computer crimes is a concern that they will expose vulnerabilities or competitive secrets during the litigation process, Congress

---

Virginia House Bill 1469, proposed on Jan. 21, 1985, as an amendment to Virginia Code Section 18.2-152.2. The Connecticut computer crime bill, Public Act 84-206, Section 2(b)(1), passed Oct. 1, 1984, uses essentially the same definition.

may wish to consider a clause that would allow some portion of the criminal proceedings to be protected. Clearly, there are trade-offs for establishing such a provision in the law, and it is important to guard against infringement of the right to an open trial. A clause that was proposed for the District of Columbia computer crime act could serve as a model.[52]

—Enacting a penalty for persons convicted of a computer crime that would include forfeiture of their interest in (i.e., confiscation of) equipment used in the crime.

A provision to this effect was included in the Administration's bill, but not in the Computer Fraud Act. The Administration argues that such a provision would be a powerful disincentive to hackers and an appropriate penalty for those who might not otherwise receive prison sentences or "meaningful fines."[53] Federal law has traditionally included only very limited forfeiture provisions, principally for drug and racketeering crimes. The effectiveness of a forfeiture provision in discouraging hacking has not been closely examined. One of the factors that would seriously hinder its effectiveness is that teenaged hackers frequently do not own the computer equipment that they use to commit a crime; adult hackers often use machines at their place of employment.

—Establishing a forum to address in a more systematic way the connections between computer crime, computer security, and Federal information policy.

The House Subcommittee on Transportation, Aviation, and Materials has recommended the formation of a national study commission to address these issues.[54] Similarly, Representative George Brown has, in several sessions, proposed the establishment of an Institute for Information Policy and Research to address national information policy issues.[55]

Such a commission or institute could help reinforce the connections between these topics, raise the visibility of a variety of information policy issues, and serve as an effective coordinator of studies, such as on the extent of computer crime. On the other hand, either a commission or an institute might delay action, and would incur some additional cost. However, proponents argue the work of a commission or institute could, in the long run, save far more than the direct cost. Several commissions have played major roles in shaping Federal policy in the issues discussed in this report, including the Commission on Federal Paperwork (which issued its final report in 1977), the panel associated with the Presidential Reorganization Project (1979), and the Privacy Protection Study Commission (1977). The first two are discussed further in chapter 2.

Any Federal effort should clearly draw from and work in concert with independent efforts in the private sector to examine these issues. For example, the American Federation of Information Processing Societies has formed a "National Information Issues Panel" to examine information policy issues and provide guidance to government leaders.[56]

---

[52] Daniel Burk, Cadwalader, Wickersham, and Taft, Washington, DC, personal communication, March 1985. The D.C. Government has not yet passed a computer crime law. The proposed clause reads in part: "The court may, in its discretion and upon good cause shown, conduct all criminal proceedings under this article in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets involved. The court's discretion under this section shall be exercised in such a way as to balance (a) the offender's important right to a public trial with (b) the District of Columbia's compelling public interests in avoiding the recurrence of the same or similar acts, in encouraging the prosecution of the crimes defined under this article, in encouraging complete and truthful testimony so that the offender is fully tried with all facts brought to the attention of the trier of fact, and in protecting the trade secrets of the owner, if any of such compelling interests are in fact present in the instant case. The court shall conduct only so much of the proceedings in secret as shall be absolutely necessary to promote these compelling interests of the District of Columbia."

[53] Toensing, op. cit.

[54] House Science and Technology Subcommittee on Transportation, Aviation, and Materials Report, "Computer and Communications Security and Privacy," April 1984.

[55] Information Science and Technology Act of 1985, H.R. 744 in the 99th Congress.

[56] American Federation of Information Processing Societies, Inc., "AFIPS Announces Formation of Panel on National Information Issues," news release, May 1985. The panel is chaired by Robert Lee Chartrand of the Congressional Research Service.

Chapter 6

Computer Modeling, Decision Support, and Government Foresight

Contents

Page

Summary 105

Introduction 106

Key Trends 108
  Information Technology Fueling Modeling Revolution 108
  Continuing Heavy Federal Use of Computer Modeling 109
  Rapidly Increasing Federal Use of Computer-Based Decision Support and Analysis 110

Key Opportunities for Action 112
  Guidelines or Standards for Model Evaluation 112
  Directory of Modeling Applications 113
  Clarified Procedures on Public Access to Modeling Details 114
  Further Research on the Development and Use of Computer Modeling and Decision Support 116
  Further Testing and Development of the Decision Conference Technique 119

Decision Support and Government Foresight 122
  Technical Advances 122
  Relevant Information 127
  Institutional Mechanisms 133

Tables

Table No. *Page*

6-1. Federal Agency Modeling Applications 110
6-2. Federal Agency Current and Planned Use of Computer-Assisted Decision Analytic Techniques 111
6-3. Illustrative Agency Formats for Model Documentation 115
6-4. Illustrative Decision Conferences Conducted by the Office of Program Planning and Evaluation, U.S. Department of Commerce, 1984-85 119
6-5. Comparison of Computer-Supported Conference Room Concepts 121
6-6. Earth-Observing Data Parameters and Applications 124

Figure

Figure No. *Page*

6-1. An Approach to Evaluating Energy (and Other) Models 126

Chapter 6

Computer Modeling, Decision Support, and Government Foresight

SUMMARY

Advances in information technology are fueling a revolution in computer modeling—both inside and outside of government. The 1980s have been characterized by the expansion of computer modeling, via low-cost microcomputers and user-friendly software, literally into the office of the individual scientist, engineer, analyst, or manager, and, simultaneously via supercomputers, to the new limits of modeling complexity demanded in the scientific, energy, space, climate, and defense sectors. The span and diversity of computer modeling activities in the Federal Government have never been greater. About 60 percent of Federal agency units responding to the OTA Federal Data Request reported at least some use of computer modeling, with the number of applications ranging up to 2,000 per agency component.

The use of computer-based decision analytic techniques has also increased dramatically. Such techniques typically include computer software that can help decisionmakers or staff analyze a specific problem, possible decision options, and the likely or possible consequences. About 90 percent of Federal agency units report use of spreadsheet software, about one-half use quantitative decision techniques (e.g., linear programming), about one-fourth use forecasting and qualitative techniques (e.g., decision trees), and a handful use decision conferences and computer-conferencing.

Overall, executive branch officials responding to the OTA Data Request believe these techniques to be very useful, even essential, to agency decisionmaking. However, few can document this claim, other than by citing ad hoc examples, because there has been little research on the impact of decision support techniques on agency decisionmaking. The limited research that is available, primarily academic research on model implementation, suggests that models (and, by extension, other decision analytic techniques) can and do have a significant impact on agency decisionmaking. Modeling may become a significant element in the process of negotiation over assumptions and options that is an integral part of agency (and, in general, political) decisionmaking. However, models can be wrong, and models can be misused.

OTA identified several possible actions that could help improve sharing of expertise and learning; facilitate public and congressional access where appropriate; enhance congressional and public understanding of the strengths and limitations, uses and abuses of modeling; and improve the government's return on a significant investment. Possible actions include:

- establishing guidelines or standards for model documentation, verification, and validation;
- establishing directories of major modeling applications;
- clarifying procedures on public and congressional access to modeling details;
- conducting further research on the impact of computer modeling and decision support on agency decisionmaking;
- conducting basic and applied research on modeling and decision support methodologies;
- conducting further testing and development of the decision conference technique; and
- bringing computer modeling and decision support clearly within the scope of information resources management.

Information technology—including data collection, archiving, and transfer, as well as modeling techniques—also makes possible improved monitoring, analysis, and, to a lesser extent, forecasting of key national and global trends. Sometimes referred to collectively as foresight capability, this potential is being facilitated by advances in:

- technical monitoring capability (e.g., through remote-sensing satellites, advanced data communication networks, and computerized data centers);
- computational and analytical capability (e.g., through the entire range of computer tools, from microcomputers to supercomputers, related software, and the procedures necessary for documenting and validating models); and
- the scientific knowledge base in the wide range of disciplines that bear on foresight.

Realization of the potential for improved foresight appears to require a synthesis of technical advances, an integration of relevant information, and institutional mechanisms that cut across agency and disciplinary lines. Many of the actions intended to improve decision support would also assist foresight, since foresight can be viewed as one component of decision support. For example, a well-developed model evaluation program built on the prior work of the National Bureau of Standards (NBS), Energy Information Administration (EIA), General Accounting Office (GAO), OTA, and others could help improve the government's modeling activities across-the-board.

The combining of computer modeling, electronic data collection, and various decision analytic techniques used in a decision conference format may be an effective technical approach to improve government foresight capability. This could involve a melding of individual techniques already in use by various government agencies, such as the White House National Security Council, Joint Chiefs of Staff, Department of Commerce's Office of Program Planning and Evaluation, and National Aeronautics and Space Administration (NASA).

OTA identified several possible actions that could facilitate improved foresight in the executive branch—ranging from bringing foresight into the scope of information resources management, planning, and innovation activities, to designating a governmentwide foresight office, either newly established or as part of an existing agency.

INTRODUCTION

In the early stages of this assessment, OTA reviewed the entire range of known applications of information technology in the Federal Government. OTA identified computer-based modeling and decision support as an applications area about which little concrete information was available. After a thorough literature search and consultation with knowledgeable persons inside and outside of the government, OTA concluded that there was no current, reliable source of information on Federal Government use of computer-based modeling and decision support. In order to develop a sound basis for understanding trends and issues relevant to computer modeling, this topic was included in the OTA Federal Agency Data Request, which was sent to all 13 cabinet departments and 20 independent agencies.

For purposes of this study, computer modeling included the entire range of mathematical models used to support agency activities and programs—from small models run on microcomputers in individual offices to large, complex models run on supercomputers. A model is an abstraction, analog, image, or representation of some aspect of current (or future) reality relevant, in this case, to the missions and programs of Federal agencies. All but the very simplest mathematical models are now routinely programmed as sets of equations and run on computers. Thus, most models are computer-based models, or computer models for short. Computer models can be used for a variety of purposes—from conducting scientific research in aeronautics or climate, to engineering the design of a new highway bridge, to estimating future numbers of school-age children, to analyzing the fiscal impacts of alternative medicare reimbursement policies. Computer models can be and are used to support agency decisions, but have many other purposes as well.

Consideration of computer-based decision support for this study included several types of analytical techniques (along with the necessary computer software, hardware, data sets, graphic displays, and the like) used to support or assist decisionmakers. The categories of computer-assisted analytical techniques used in the OTA Federal Agency Data Request and in this chapter are:

- spreadsheet computer software;
- forecasting techniques (e.g., regression analysis, Delphi survey);
- quantitative decision analytic techniques (e.g., linear programming, queuing analysis, systems analysis, critical path analysis);
- quantitative decision analytic techniques with judgmental input (e.g., decision trees, subjective probability, multi-attribute utility).
- decision conference techniques (e.g., interactive use of computer-assisted analytical techniques by decisionmakers in a group situation);
- electronic voting techniques (e.g., consensor, computer polling);
- computer-conferencing for decision analysis; and
- other (e.g., expert systems).

Most of these techniques also involve the use of models. For example, an analysis of the relationship between rainfall, temperature, and crop yield might use a computer-based multiple regression model to better understand the performance of different varieties of crops (e.g., wheat) under various climatic conditions, or to help an agricultural extension agent or Agency for International Development agricultural employee select specific varieties to recommend for spring planting.

This chapter presents OTA's findings on key trends and issues relevant to computer modeling and decision support. In addition, it discusses the potential for improved government foresight through the use of information technology and decision support techniques. One objective of foresight is to help government decisionmakers better understand and consider longer term trends and implications when making decisions. From that perspective, foresight can be properly viewed as part of decision support.

Realization of the potential to improve government foresight appears to require a synthesis of technical advances, an integration of relevant information, and institutional mechanisms that cut across agency and disciplinary lines. The foresight portion of this chapter extends the earlier discussion of computer modeling and decision support to include:

- remote-sensing satellites for collecting foresight-related data;
- model evaluation procedures for foresight-related computer models;
- systems science for analysis of complex trends and issues relevant to foresight;
- data integration and display techniques, with examples from NASA, the National Security Council, and the Joint Chiefs of Staff;
- advanced decision support techniques that could be applied to foresight; and
- institutional mechanisms, both agency-specific and governmentwide, that could help facilitate improved foresight.

The major foresight sectors can be viewed as spanning the entire range of Federal Government programs and activities, including, for example: energy, environment, water, climate, food, population, transportation, housing, education, the economy, foreign trade, and national security. Not all techniques are equally applicable to all foresight sectors. Thus, for example, remote-sensing satellites are most applicable to the environmental and natural resources (e.g., including food, water, climate, land use) sectors of foresight. Large-scale modeling is most applicable to those sectors, such as energy and climate, where key variables and relationships can be quantified and where substantial input data are available. On the other hand, some decision analytic techniques (e.g., decision conferences, computer-conferencing) are applicable to both quantitative and qualitative, observational and judgmental information, and thus are relevant to many, if not all, foresight sectors.

KEY TRENDS

Information Technology Fueling Modeling Revolution

Several key technological developments have profoundly changed the conduct of analytical, forecasting, and research activities that utilize modeling. The first is the microcomputer revolution. This study has documented elsewhere the exponential increase in microcomputers in the Federal Government. From almost no microcomputers 10 years ago to only a few thousand 5 years ago, Federal agencies now have, collectively, more than 100,000. Access to computer power truly has been decentralized, both in terms of actual desktop computer capability and the use of microcomputers as access points to larger mainframe computer resources. This phenomenon parallels that found in the research and business communities outside of government.

A second key trend is the large increase in user-friendly computer software, especially software suitable for microcomputers. This includes a wide range of spreadsheet, modeling, and decision analytic software that permits many small-scale, relatively simple decision analytic and modeling applications.

A third key technological trend is at the high end of computer power—the supercomputer. Supercomputers are extending the limits of modeling complexity, whether it be in aerodynamics, high-energy physics, or climate. In the United States, supercomputers have been installed at, for example, the Lawrence Livermore Laboratory (Department of Energy) for magnetic fusion research, and at the Ames Research Center (NASA) for numerical aerodynamics modeling. Both NASA and the Department of Energy (DOE) officials have stated that supercomputers are essential to their modeling activities.[1]

Use of supercomputers is not limited to government agencies. For example, with National Science Foundation (NSF) funding, additional supercomputer centers are being established at several universities—including the University of California at San Diego, Cornell University, Princeton University, and the University of Illinois at Urbana-Champaign—to augment universities such as Purdue and Minnesota that already had supercomputers. At Illinois, illustrative anticipated applications range from high energy physics (e.g., simulation of a particle accelerator to test theories about elementary particles), to chemistry (e.g., simulation of molecular behavior), to civil engineering (e.g., modeling of transportation systems in the Chicago area), to physiology and biophysics (e.g., modeling of electrical activity of nerve and muscle cells).[2]

The earliest computer modeling dates back to the 1950s when first-generation computers were used, for example, to run simple numerical models for weather prediction. Until around 1970, Federal Government modeling was concentrated in the scientific, energy, space, and defense sectors—sectors with the greatest computational needs and the resources to pay for the expensive but necessary computer power. During the decade of the 1970s, however, the widespread availability of relatively cheap computers contributed to the expansion of computer modeling activities to areas such as air pollution, water resources, solid waste management, urban development, and transportation. The 1980s have been characterized by the expansion of computer modeling, via low-cost microcomputers, literally into the office of the individual scientist, engineer, analyst, or manager, and, simultaneously via supercomputers, to the new limits of modeling complexity demanded in, for example, the energy and climate sectors.[3] The results of OTA's Federal Agency Data Request (presented later) indicate that the span and diversity of computer modeling activities in the Federal Government have, without question, never been greater.

---

[1] See Frank R. Bailey, "NAS: Supercomputing Master Tool for Aeronautics," *Aerospace America*, January 1985, pp. 118-121; June Altman, "Cray-2 Called Super in Memory, Performance," *Management Information Systems Week*, June 12, 1985, p. 12; Don Dagani, "Supercomputers Helping Scientists Crack Massive Problems Faster," *Chemical and Engineering News*, Aug. 12, 1985, pp. 7-13; and James Connolly, "Cray Doubles Memory On X-MP Line," *Computerworld*, Sept. 23, 1985, p. 4.

[2] Judith Axler Turner, "Supercomputer Raises Expectations Among Researchers at University of Illinois," *The Chronicle of Higher Education*, Oct. 23, 1985, p. 24. Also see U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues*, OTA-CIT-268 (Washington, DC: U.S. Government Printing Office, February 1985).

Weather and climate modeling is a good illustration of how computer modeling in general has essentially developed in parallel with advances in computer power. The record shows that the complexity of weather and climate models quickly expands to push the limits of the computational power and capacity of each successive generation of computer technology.[4]

Continuing Heavy Federal Use of Computer Modeling

Federal agency use of computer modeling is substantial—almost 60 percent of 141 agency components responding to the OTA Data Request reported some use of computer modeling to support of agency activities and programs. And this excludes use of decision analytic techniques such as spreadsheet software discussed in the next section. (Note: The OTA Data Request was limited to the Federal executive branch. Other OTA research reviewed use of computer modeling by Congress[5] and State legislatures.[6] See the discussion in ch. 8.)

For agencies that could estimate the total number of modeling applications, the number ranged up to 2,000 per agency component. Among the heaviest reported computer model users are the Economic Research Service (Department of Agriculture), Office of Program Analysis and Evaluation (Department of Defense (DOD)), U.S. Geological Survey (Department of the Interior), Federal Highway Administration (Department of Transportation (DOT)), and the Nuclear Regulatory Commission (NRC).

OTA asked agency components to list the 10 heaviest areas of modeling application. The results demonstrated the wide diversity in the purposes for which computer modeling is used by Federal agencies. Examples from seven selected agencies are shown in table 6-1.

Although the results of the OTA Federal Agency Data Request are not adequate to make a precise estimate of the number of modeling applications, it is clear that the total is far higher than previously thought. A 1982 GAO survey identified 357 models used in the agency policymaking process, based on responses from 12 of the 13 cabinet departments and 18 independent agencies.[7] The GAO survey very likely underreported the total number of policy-relevant models as of that time (1982), and the number has probably increased since then. While a precise estimate is neither possible or necessary, the ballpark *minimum* would appear to be in the thousands for policy models and tens of thousands for all types of computer models used by Federal agencies.

---

[3] See Saul I. Gass and Roger L. Sisson, *A Guide to Models in Governmental Planning and Operations*, report by Mathematica, Inc., prepared for U.S. Environmental Protection Agency, August 1974; and OTA, *Information Technology R&D*, op. cit., pp. 57-61.

[4] The original numerical weather forecast models were run on first-generation mainframe computers (e.g., IBM 701) in the 1950s, and the original atmospheric general circulation models on second-generation computers (e.g., IBM 7094) in the 1960s. The first global coupled atmosphere-ocean model was run in the mid-1970s on the state-of-the-art third-generation computers (e.g., IBM 360-195). (U.S. National Academy of Sciences, National Research Council, U.S. Committee for the Global Atmospheric Research Program, *Understanding Climate Change: A Program for Action*, Washington, DC, 1975, pp. 198-201.)

Today, the most complex climate models are straining the capability of class VI supercomputers (e.g., Cray-1 or Cyber 205) and are providing the impetus for climate modelers to move up to even more powerful supercomputers. (National Center for Atmospheric Research, *Annual Report Fiscal Year 1984*, NCAR/AR-84, Boulder, CO, March 1985, p. 36.)

[5] Stephen E. Frantzich, "Congressional Applications of Information Technology," OTA contractor report prepared by Congressional Data Associates, February 1985.

[6] Robert Miewald, Keith Mueller, and Robert Sittig, "State Legislature Use of Information Technology in Oversight," OTA contractor report prepared by the University of Nebraska-Lincoln, January 1985.

[7] U.S. General Accounting Office, *Survey to Identify Models Used by Executive Agencies in the Policymaking Process*, GAO/PAD-82-46, Sept. 24, 1982.

Table 6-1.—Federal Agency Modeling Applications

Economic Research Service (Department of Agriculture)
An estimated 2,250 computer modeling applications, including:
- analysis of farm program alternatives
- analysis of world food supply, capacity, and response
- analysis of conservation alternatives
- trade policy analysis
- forecasting of commodity supply and demand

Forest Service (Department of Agriculture)
An estimated 100 applications, including:
- timber resource allocation model
- integrated pest impact assessment system
- forest growth and yield analysis
- fire management and planning model
- engineering design models for roads, structures, and buildings

Office of Secretary of Defense (Office of Program Analysis and Evaluation)
An estimated 1,250 applications, including:
- impact of defense spending on U.S. economy
- strategic defense initiative effectiveness studies
- military force mobility modeling
- impact of procurement schedule changes on acquisition costs
- impact of second-source/competitive procurement on acquisition costs

Joint Chiefs of Staff (Department of Defense)
A large number of applications, including:
- strategic nuclear war plans analysis
- non-strategic nuclear force mix analysis
- military force posture analysis
- improving crisis war planning processes
- nuclear damage assessment

Bureau of Indian Affairs (Department of the Interior)
An estimated 15 applications, including:
- road and bridge design
- forest and range fire risk analysis
- rangeland usage and conditions analysis
- rangeland market appraisal
- oil and gas lease management and planning

Office of Assistant Secretary for Program Evaluation (Department of Health and Human Services)
A small number of applications, including:
- revenue impact analyses of, for example, including social security and welfare benefits in taxable income, providing additional tax exemptions for children in the first year after birth, and replacing Federal income tax credits for the elderly with higher deductions.
- estimates of participation rates for Aid for Dependent Children (AFDC) recipients in the Food Stamp Program.
- estimates of the Deficit Reduction Act impact on AFDC, Food Stamp, and Supplemental Security Income beneficiaries.

Federal Emergency Management Agency
An estimated 100 applications, including:
- mobilization for nuclear and general war
- earthquake damage and economic impact estimates
- residual capacity of U.S. economy after nuclear war
- strategic stockpile policy development
- flood damage analysis

SOURCE: Office of Technology Assessment Federal Agency Data Request

The numbers could be much higher, especially if spreadsheet-type models are included.

Rapidly Increasing Federal Use of Computer-Based Decision Support and Analysis

Computer-based decision analysis, per se, dates back to the 1960s for its theoretical roots (e.g., as developed by Howard Raiffa of Harvard University),[8] and to the 1970s for its practical development and early application—primarily in the military and business sectors. Early Federal Government sponsors of research and development (R&D) on decision analysis included the Defense Advanced Research Projects Agency and the Office of Naval Research. The early decision analytic tools were implemented with paper and pencil, slide rule, and/or calculator.

Since decision analysis techniques may involve many options (e.g., numerical probabilities based on empirical evidence and/or quantified judgments of uncertain future events), the number of calculations per run can be large, and the typical application involves many runs with changing options and values. Thus, decision analysis is a natural match with electronic computer capability. Therefore, almost all decision analytic techniques are significantly if not entirely run on computers, at least for the computational aspects. Many decision analysis software packages are now available off-the-shelf for use on microcomputers, and the software and hardware, together with relevant databases, are frequently known as decision support systems.

The results of the OTA Federal Agency Data Request provided a good profile of agency use of decision analytic techniques—the first complete profile known to exist. The results are likely to understate the full extent of use, given the highly decentralized nature of decision support. Nonetheless, the results are generally consistent with the perceptions of informed observers, especially with respect to the relative differences in levels of use for the various techniques.

---

[8] Howard Raiffa, *Decision Analysis*(Reading, MA: Addision-Wesley, 1968). Also see Rex V. Brown, "A Brief Review of Executive Agency Uses of Personalized Decision Analysis and Support," OTA contractor report prepared by Decision Science Consortium, Inc., March 1985.

The results are summarized in table 6-2. As shown, spreadsheet software is used by almost all (88 percent) of the agency components responding, and half of the remaining agency components (8 out of 16) are planning to use spreadsheet software. Almost half (47 percent) of agency components report the use of quantitative decision analytic techniques, with another 13 agency components planning to use such techniques. About one-fifth (22 percent) of agency components report use of quantitative decision analytic techniques with judgmental input, and about one-fifteenth report use of decision conference techniques. Nine agency components report use of decision conferences, and another seven components indicate that they are planning to do so. About one-twentieth report use of computer-conferencing for decision support, and two agency components indicate use of electronic voting techniques. Also, three components report planned use of expert systems or artificial intelligence for decision support.

Use of spreadsheet software is spread throughout all agencies, and use of quantitative techniques is fairly widespread in, for example, the Departments of Agriculture, Commerce, Defense, Interior, Transportation, Treasury, and about two-thirds (12 of 19) of the independent agencies surveyed. However, DOD is the only agency with more than half of agency components reporting use of quantitative decision analytic techniques with qualitative input (e.g., decision trees, multiattribute utility). Likewise, DOD is the only agency reporting significant use of decision conferences (about one-third of DOD components reporting), although there was very scattered, infrequent use reported in Agriculture, Interior, and Transportation.

With respect to use of quantitative decision analytic techniques, the International Economic Policy (IEP) Group of the International Trade Administration (Department of Commerce) is illustrative. This agency component combines the use of decision analytic techniques, models, and databases "to help improve decisionmaking" and "to enhance IEP's ability to provide policymakers and U.S. business with comprehensive information on trade and investment matters generally." As one other agency example, the Drug Enforcement Administration (DEA) (Department of Justice) is planning to use quantitative decision techniques to optimize allocation of agency resources (agents, monies for purchase of information and evidence, etc.) in terms of pro-

Table 6-2.—Federal Agency Current and Planned Use of Computer-Assisted Decision Analytic Techniques

	Current use[a]					Planned use[b]
	Yes		No		Total	
Technique	No.	%	No.	%	No.	No.
Spreadsheet software (e.g., Lotus 1-2-3, VisiCalc)	121	88.3	16	11.7	137	8
Quantitative decision analytic techniques (e.g., linear programming, queuing analysis, systems analysis, critical path analysis)	64	47.4	71	52.6	135	9
Forecasting techniques (e.g., Delphi, regression analysis)	33	24.6	101	75.4	134	13
Quantitative decision analytic techniques with judgmental input (e.g., decision trees, subjective probability, multi-attribute utility)	29	22.1	102	77.9	131	10
Decision conference techniques (e.g., interactive use of computer assisted analytical techniques by decisionmakers in group situation)	9	6.8	124	93.2	133	7
Computer-conferencing for decision analysis	6	4.6	124	95.4	130	4
Electronic voting techniques (e.g., consensor)	2	1.5	132	98.5	134	1
Other: Expert Systems, artificial intelligence						3

[a] Agency components reporting current use

[b] Agency components reporting planned use of techniques not currently used.

SOURCE: Office of Technology Assessment, based on results of Federal Agency Data Request.

ductivity as measured, for example, by the number of repeat offender arrests, volume and value of drug interdictions, and reductions in drug availability. Also, DEA plans to use quantitative techniques with judgmental input and artificial intelligence techniques for investigative and intelligence purposes.

Other examples of the use of decision analytic techniques, especially those combining quantitative and qualitative (judgmental) methodologies, include:

- DOD use of multi-attribute utility analysis to aid in the evaluation and acquisition of major military systems such as the Advanced Scout Helicopter, Light Armored Vehicle, Mobile Protective Weapons System, and Single Channel Ground and Airborne Radio System;
- Defense Nuclear Agency use of multi-attribute utility and cost-effectiveness analysis to aid in R&D budgeting;
- Department of the Air Force use of decision analytic techniques to aid in planning and targeting air strikes against enemy air bases, and in developing command, control, and communication countermeasures;
- NRC use of decision analysis to aid in evaluation of proposed new regulatory requirements and safeguard designs;
- DOE use of decision analysis to aid in implementation of the Nuclear Waste Policy Act of 1982 and the siting of repositories for high-level nuclear waste;
- National Security Council use of decision analysis in evaluating alternative strategies for the Middle-Eastern region; and
- President's Council on International Economic Policy use of decision analysis in evaluating alternative export control policies for computer technology.

For further discussion of these and other applications, see the OTA contractor reports prepared by Decision Science Consortium, Inc., listed in appendix C.

KEY OPPORTUNITIES FOR ACTION

Guidelines or Standards for Model Evaluation

Efforts to manage computer modeling and to establish some minimum level of standards have always lagged behind the actual level of applications by many years. In the 1970s, as computer modeling applications proliferated throughout the Federal Government, the National Bureau of Standards, Energy Information Administration, and the General Accounting Office took the lead in attempting to bring some coordination and coherence to civilian modeling activities. The Joint Chiefs of Staff (JCS) did likewise for defense modeling.

GAO issued reports in 1976, 1978, and 1979, and NBS issued reports in 1979 and 1981 (with EIA support).[9] A central theme in all of these reports was the need to develop some kind of common framework for model evaluation or assessment. Many suggestions were made, but none were adopted on a governmentwide basis. A very few individual agencies, such as EIA, eventually adopted some variant of a model evaluation procedure. (For further discussion of EIA model documentation and evaluation, see table 6-3 and related discussion below under the topic of public access to modeling details.)

Given the very extensive use of computer modeling by Federal agencies, the level of formal model documentation, verification, and validation appears to be deficient. Clearly, computer models are judged to be important by many Federal agencies and are used for purposes ranging from research to decision support. However, the research on computer modeling makes two things abundantly clear: models can be wrong, and models can be misused.[10] For these reasons alone, minimum modeling guidelines or standards appear to be needed. In addition, such guidelines presumably would make it easier to strengthen the Federal modeling expertise, and, hopefully, achieve a higher return on what must be a substantial Federal investment. (OTA did not develop data on the costs of modeling, and most agencies are unable to readily estimate such costs.)

---

[9] U.S. General Accounting Office, *Ways To Improve Management of Federally Funded Computerized Models*, Aug. 23, 1976; *Models and Their Role in GAO*, October 1978; *Guidelines for Model Evaluation*, January 1979; U.S. Department of Commerce, National Bureau of Standards, *Utility and Use of Large-Scale Mathematical Models*, Saul I. Gass (ed.), May 1979; *Validation and Assessment of Energy Models*, Saul I.Gass (ed.), October 1981.

As noted above, some agencies (e.g., NBS, EIA, JCS) have made a concerted effort to develop and/or apply modeling guidelines. A lead role could be assigned to one of these agencies, perhaps NBS, or to one civilian and one military agency (e.g., NBS and JCS), for developing and promulgating a set of modeling guidelines. Much of the groundwork has already been done, and development of guidelines should be straightforward.[11] The lead agency would presumably involve all major modeling agencies in the guidelines development process. Guidelines for the major, expensive, complex computer models would logically be more complete and extensive than guidelines for small, simple, inexpensive, desktop models. Computer modeling could be brought clearly within the purview of the information resources management concept, through appropriate amendments to the Paperwork Reduction Act if necessary.

Directory of Modeling Applications

Prior studies of computer modeling in the Federal Government have generally concluded that directories of modeling applications would be helpful—at least for the major models. This possibility was reiterated in a 1982 OTA study on water resources models.[12] Given the extremely large number of applications, a comprehensive directory would appear to be costly and difficult to prepare, and many of the applications simply may not warrant the effort. However, there is a stronger argument for a comprehensive directory of selected major models and for an index or pointer system to a larger number of other significant models and modelers, perhaps indexed by subject matter and type of model. These actions would be intended to help reduce possible excessive overlap and duplication, encourage exchange of modeling information among modelers, and facilitate a greater degree of public knowledge of and access to Federal modeling. Some argue that modelers in any given area already know or can learn what they need to know about relevant modeling activities without the help of modeling directories. But given the number and diversity of modeling applications, this could be difficult.

Of 82 agency components that reported use of computer models, 16 or about one-fifth indicated the existence of a modeling directory. Those agencies are:

Department of Agriculture:
—Economic Research Service
—Forest Service
Department of Defense:
—Joint Chiefs of Staff
—Defense Contract Audit Agency

---

[10] See, for example, Brian Wynne, "The Institutional Context of Science, Models, and Policy: The IIASA Energy Study," *Policy Sciences*, vol. 17, No. 3, November 1984, pp. 277-320; W. Hafele and H.H. Rogner, "A Technical Appraisal of the IIASA Energy Scenarios? A Rebuttal," *Policy Sciences*, vol. 17, No. 4, December 1984, pp. 341-365; Bill Keepin and Brian Wynne, "Technical Analysis of IIASA Energy Scenarios," *Nature*, vol. 312, December 1984, pp. 691-695; and David Dickson, "Global Energy Study Under Fire," *Science*, vol. 227, January 1985, p. 4. For a discussion of errors in forecasting models, see William Ascher, *Forecasting: An Appraisal for Policymakers and Planners* (Baltimore, MD: Johns Hopkins University Press, 1978). For discussion of limitations and risks associated with computer-based planning and forecasting techniques, see Charles Stubbart, "Why We Need a Revolution in Strategic Planning," *Long Range Planning*, vol. 18, No. 6, December 1985, pp. 68-76; Henry Petroski, "Superbrain, Superrisk," *Across the Board*, vol. 12, No. 12, December 1985, pp. 48-53; and Kennedy Maize, "How It Didn't Turn Out: The Forecasters Who Failed (And One Other)," *The Energy Daily*, vol. 14, No. 1, Jan. 2, 1986.

[11] See, for example, GAO, *Guidelines*, op. cit.; NBS, *Utility*, op. cit.; and GAO, *Validation* op. cit.; Richard Richels, "Building Good Models Is Not Enough," *Interfaces*, vol. 11, No. 4, August 1981, pp. 48-51; and Saul I. Gass and Lambert S. Joel, "Concepts of Model Confidence," *Computers and Operations Research*, vol. 8, No. 4, 1981, pp. 341-346.

[12] U.S. Congress, Office of Technology Assessment, *Use of Models for Water Resources Management, Planning, and Policy* (Washington, DC: U.S. Government Printing Office, August 1982).

Department of Energy:
—Energy Information Administration
Department of the Interior:
—Minerals Management Service
—U.S. Geological Survey
—Office of Surface Mining Reclamation and Enforcement
Department of Justice:
—Justice Management Division
Department of Labor:
—Bureau of Labor Statistics
Department of Transportation:
—National Highway Traffic Safety Administration (NHTSA)
—Federal Highway Administration
—Federal Aviation Administration
Nuclear Regulatory Commission
Arms Control and Disarmament Agency
Federal Emergency Management Agency

Most of these directories are reported to be in paper format, although the Forest Service and NHTSA indicate that their directories are in an on-line electronic format. Also, the EIA model directory is in both computerized and printed formats.

In addition, some of these agency components report that they also have a central reference point—usually a designated person—with current information about modeling applications. Several other agency components that do not have a directory do claim to have a contact person. Among the latter agencies are, for example, the Defense Advanced Research Projects Agency, Defense Communications Agency, Department of Energy agencywide (National Energy Software Center—a full clearinghouse operation, not just a person), Employment Standards Administration (Labor), Urban Mass Transit Administration (DOT), and Comptroller of the Current (Treasury).

In total, a little more than one-third (31 out of 82) of the agency components that use computer modeling report having a model directory and/or a designated contact person or, rarely, an actual clearinghouse. This one-third includes many of the agency components that appear to be among those with the heaviest modeling activity. These figures do not include model directories or clearinghouses that include Federal agency models but are maintained by non-Federal entities (e.g., universities, professional associations, and private information companies).

With respect to decision analytic support, only five agencies reported a directory or clearinghouse of such applications. The decentralized and small-scale nature of most decision analytic applications probably makes a directory to these techniques unrealistic.

However, for major modeling applications—such as the major energy, agriculture, water, transportation, and climate models—a directory appears to make sense. Such a directory or family of directories should be useful to all parties concerned—Congress, the public, agency modelers, researchers, and the like. Several prototypes exist. The directories would logically be computerized, to facilitate easy updating, and could be available in on-line electronic format as well as in paper and microform. A common table of contents would be helpful, and would presumably be consistent with whatever modeling guidelines may be developed. The directories could be organized by—at a minimum—agency, subject area, and type of modeling application (e.g., scientific research, decision support, program implementation) to facilitate easy reference.

A lead agency could be designated, perhaps the NBS Center for Operations Research and/or the NBS Institute for Computer Science and Technology, to study the options and develop a feasible directory design. The modeling directories and contact persons reported to OTA by the agencies should provide a good base from which to start.

Clarified Procedures on Public Access to Modeling Details

Only about one-tenth of agency components using computer modeling have formal procedures or policies (beyond the Freedom of Information Act) on the availability of modeling details (e.g., structure, assumptions, input data) to the public and Congress, and there is wide variability among the procedures and policies that do exist.

The overall results indicate that most agencies have not given much attention to questions of public and congressional access to model details. Some agencies cite the Freedom of Information Act as the guiding policy; others state that modeling details would probably be provided if sought by Congress.

The following agencies indicated the existence of procedures or policies on the availability of model details to the public and/or Congress:

- Economic Research Service (ERS) (Agriculture)
- Bureau of the Census (Commerce)
- Joint Chiefs of Staff (Defense)
- Energy Information Administration (Energy)
- U.S. Geological Survey (Interior)
- Bureau of Labor Statistics (BLS) (Labor)
- Urban Mass Transportation Administration (Transportation)
- Federal Aviation Administration (Transportation)
- Nuclear Regulatory Commission

Most of the major Federal statistical agencies are included in the above list (e.g., ERS, Census, EIA, BLS) because they use models in developing statistical trends and forecasts and because there is a highly visible public demand for their information products. Thus, there is a strong felt need to develop explicit access policies.

However, even among the few agencies that have explicit policies, there is considerable variability in the level of public documentation that is routinely made available. This does not appear to necessarily reflect an agency judgment to actively withhold certain kinds of modeling information, but appears to be more a reflection of the particular approach selected for model documentation. Examples from three agencies are presented in table 6-3.

The EIA public documentation of major models is one of the most extensive of all agencies responding to the OTA Data Request. This is partly attributable to the high visibility of energy modeling over the last decade or so, periodic concerns raised about the quality of EIA energy models and projections, and congressional and statutory requirements. For

Table 6-3.—Illustrative Agency Formats for Model Documentation

Economic Research Service (Department of Agriculture)[a]
- Model name
- Responsible person(s)
- Model description
- Model applications
- Operating and updating costs

Joint Chiefs of Staff (Department of Defense)[b]
- Model title
- Model type
- Proponent (who maintains model)
- Developer
- Purpose
- General description
- Date implemented
- Input
- Output
- Model limitations
- Hardware
- Software
- Time requirements
- Security classification
- Frequency of use
- Users
- Point of contact
- Miscellaneous
- Keyword listing

Energy Information Administration (Department of Energy)[c]
- Model name
- Acronym
- Abstract
- Status
- Part of another model
- Sponsoring agency, office, division, branch
- Model contact
- Documentation
- Archive tape(s) and installation manual(s)
- Reviews conducted (of model)
- Purpose
- Energy system described by model
- Coverage (e.g., geographic, time unit/frequency)
- Special features
- Modeling features
  - —Model structure
  - —Modeling technique
  - —Model interfaces
  - —Input data
  - —Date sources
  - —Output data
- Computing environment
  - —Language used
  - —Core memory requirements
  - —Estimated cost to run
  - —Special features
- Status of evaluation efforts
- Date of last model update

---

[a] See U.S. Department of Agriculture, Economics and Statistics Service, *Agriculatural and Other Economic Models of the Economics and Statistics Service*, April 1981. According to USDA personnel, this document is still relatively current, and no update has been scheduled.

[b] Joint Chiefs of Staff, Joint Analysis Directorate, "Memorandum for Agencies and Organizations Involved in Wargaming and Military Simulation Modeling," re: "Catalog of Wargaming and Military Simulation Models," June 1, 1984.

[c] U.S. Department of Energy, Energy Information Administration, *Directory of Energy Information Administration Model Abstracts*, Feb. 1, 1985.

example, EIA has a statutory mandate to insure "that adequate documentation for all statistical and forecast reports prepared . . . is made available to the public at the time of publication of such reports."[13] Since many such EIA reports are based on computer models, the models themselves are required to be documented. EIA has issued two orders that specify the format and public availability of model documentation.[14] In addition, in part in response to congressional criticism and outside audits and evaluations, it appears EIA has made significant progress in documenting the 33 major computer models currently in use, of which 24 are so-called basic models.[15] EIA has made extensive use of model evaluations conducted by outside groups, as well as internal reviews.

The EIA and JCS model documentation illustrated above provide considerably more information than the ERS format, since the latter is really a pointer system to help interested parties obtain more detailed information if desired. However, ERS also publishes reports on some of the major models. For example, a report on the ERS "World Grain-Oilseeds-Livestock Model" is 64 pages long and includes a narrative description, illustrations of model equations and linkages, and values of key model parameters.[16] This report is backed up by an even longer technical report also prepared by ERS staff. This suggests that, even if modeling information available through directories or other "public access" mechanisms is limited, more detailed information may be available through technical reports prepared by agency (and/or consultant) staff and also via articles in the published literature. Even the EIA's detailed public documentation is only an "abstract" of more extensive information available from knowledgeable EIA personnel.

As noted above, the agencies that use computer models to support major public information products (e.g., statistical reports on forecasts) generally have established means to make modeling information available. However, other agencies have not explicitly dealt with the access question. Some simply recite the Freedom of Information Act. Others suggest that information would be made available if requested. There may not be a real issue here, except to the extent that modeling and decision support information is considered classified (primarily with respect to military applications) or subject to executive privilege. Public access to models developed by government contractors can also be a problem. The public availability of such information appears to need clarification. Also, the current central access mechanisms (e.g., the National Technical Information Service and the National Energy Software Center) could be reviewed for adequacy and possible modification.

Further Research on the Development and Use of Computer Modeling and Decision Support

Judging from the apparent extensive use of computer models and the positive tone of agency comments, computer models and decision support do have a significant impact on agency decisionmaking. For example, the Antitrust Division of the Department of Justice, and in particular the Economic Policy Office, stated that:

> . . . [t]he data manipulation and sophisticated economic and statistical analyses now used in connection with almost all matters could not be performed without computers. While it is impossible to estimate savings in staff time by using computer support, such savings are clearly large.

---

[13] Public Law 93-275, Section 57(B)(1) as amended by Public Law 94-385.

[14] See Energy Information Administration Order No. E15910.3A, "Guidelines and Procedures for Model and Analysis Documentation," Oct. 1, 1982, and Order No. E15910.4A, "Guidelines and Procedures for the Preparation of Model Archival Packages," Feb. 23, 1982.

[15] See Energy Information Administration, *Directory of Energy Information Administration Model Abstracts*, Feb. 1, 1985; and Professional Audit Review Team, *Performance Evaluation of the Energy Information Administration*, report to the President and Congress, June 15, 1984, which noted significant progress on model documentation but with additional work still needed.

[16] Karen Liu and Vernon O. Roninger, *The World Grain-Oilseeds-Livestock (GOL) Model, A Simplified Version*, ERS Staff Report No. AGE5850128, U.S. Department of Agriculture, Economic Research Service, International Economics Division, February 1985.

Nonetheless, the results of the OTA Federal Agency Data Request suggest that the actual use of models for decisionmaking has received little systematic study by Federal agencies. Very few (about 4 percent) of the agencies using computer models report having conducted or sponsored such studies. Likewise, about 7 percent of agencies using decision support report having conducted or sponsored studies.

Of the few agencies that were able to provide concrete examples of studies, only the Federal Emergency Management Agency (FEMA) documented a clearly relevant study program (being carried out both in-house and with NBS assistance). It is likely that some study programs also exist in other agencies, especially in DOD components, but that the details or even the existence of such studies are unknown to headquarters personnel. The responses of the Army, Navy, and Air Force headquarters noted the decentralized nature of agency operations, which makes it difficult, absent a major data collection effort, to be fully knowledgeable about prior or ongoing studies. On the other hand, neither the Joint Chiefs of Staff nor the Program Analysis and Evaluation Office (in the Office of the Secretary of Defense) indicated any such studies even though these two components make heavy use of computer models. It is possible that such studies may be classified, although no indication to this effect was made to OTA by knowledgeable DOD personnel.

JCS staff state that no such studies are conducted because the substantial value of computer modeling is clear and undisputed and, in any event, evaluation studies would be difficult to do, given the multiple factors that affect JCS decisions. Computer model results are just one input among many.

On the other hand, FEMA has made a major commitment to evaluate its computer models, many of which are intended to support planning for, and decisionmaking under, emergency conditions. For example, in 1982, FEMA prepared a 130-page report of the FEMA Modeling Task Force that outlined a comprehensive plan for review and evaluation of FEMA modeling and analytical activities.[17] In 1984, reports were issued on various FEMA models, including the:

- dynamic general equilibrium model designed to simulate economic conditions before and after an emergency, including nuclear attack, general wartime mobilization, and other severe economic disruptions[18]; and
- damage assessment model designed to estimate the effects of a nuclear attack on various critical resources such as livestock, crops, housing, hospitals, and physicians.[19]

These and other models are then to be evaluated within a framework developed by the Center for Applied Mathematics of NBS under contract to FEMA. The evaluation procedure is intended to, among other things, test the extent to which a model meets user requirements. NBS has identified a wide range of analytical techniques for model evaluation, including:[20]

- descriptive analysis (e.g., motivation of model, theoretical underpinnings, model development);
- program verification and analysis (e.g., review of documentation and source code, model implementation);
- data audit (e.g., review of documentation, analysis of computerized files);
- sensitivity analysis (e.g., error analysis, statistical analysis, model stability); and
- program usability (eg., user-model interface, maintenance and update procedures).

This latest NBS effort for FEMA represents a continuation of and builds on earlier work conducted in part for EIA, and could very well serve as a prototype for other agencies.

---

[17] Bruce J. Campbell, Task Force Chairman, "FEMA Modeling Task Force Study," FEMA, May 1982.

[18] Richard J. Goettle III and Edward A. Hudson, *Final Report on the Dynamic General Equilibrium Model*, prepared for FEMA under contract FPA 76-9, February 1984.

[19] FEMA, *Ready II Damage Estimation System Advanced Analytical Programs*, TM-308, February 1984.

[20] Robert E. Chapman, Robert G. Hendrickson, Saul I. Gass, and James J. Filliben, *Analytical Techniques for Evaluating Emergency Management Models and Data Bases*, prepared by NBS Center for Applied Mathematics under contract to FEMA, May 1985.

Beyond this, there is a considerable body of research and discussion in the published academic and scholarly literature,[21] popular and trade press,[22] and various research reports, for example, those sponsored by NSF on the use of models and decision analysis in risk assessment.[23] Also, variants of computer modeling and decision analysis are being used in the development of computer-based expert systems and artificial intelligence.

In sum, however, while many agencies believe in the utility of computer modeling and decision analytic techniques, few apparently think that studies are worth the time and resources. Nonetheless, it seems highly unlikely that all agencies are making the best and most cost-effective use of such techniques. A coordinated, modest research program could help illuminate what kinds of techniques and applications are working well and which are not. The results of such research would presumably facilitate the exchange of knowledge about computer modeling and decision support, and lead to improved cost-effectiveness. The results would also be helpful to the development of model guidelines (discussed above).

In addition to encouraging and funding research, other mechanisms for sharing knowledge could be encouraged, such as professional forums for model developers and users (as has been tried in, for example, the energy and water resource modeling areas), and additional training opportunities.

The limited research that is available, primarily academic research on model implementation, suggests that models (and, by extension, other decision analytic techniques) can and do have a significant impact on agency decisionmaking. Models may become a significant element in the process of negotiation over assumptions and options that is an integral part of agency (and, in general, political) decisionmaking. However, models can be misused and abused. It may be important to understand the models and their roles in order to understand the ultimate decision.[24]

From this perspective, then, the results of further research may provide some new insights as to what kinds of questions should be asked and information requested in conducting oversight on agency decisions, and what kinds of techniques might be useful in program evaluations and audits conducted by GAO and others.

GAO and agency program evaluation and audit offices are generally very active and looking for ways to improve evaluation and audit methodologies. Indeed, GAO is required, by the Congressional Budget Act of 1974, to monitor and recommend improvements in program and budget information for congressional use. GAO has, for example, identified needed improvements in DOD's planning, programming, and budgeting system, in the Environmental Protection Agency's cost-benefit analyses of environmental regulations, and in DOD's procedures for estimating weapons system costs.[25] In all these areas, decision analytic techniques have a potential role, especially techniques that combine quantitative and qualitative information, identify ranges of uncertainty, and specify the nature and extent of subjective value judgments to the extent present in the analysis. GAO and other audit agencies could experiment with such decision analytic techniques to ascertain their potential to improve program and budget information for congressional use.

---

[21] For further discussion of the history and techniques of decision analysis, see, for example, R.V. Brown, A.S. Kahr, and C. Peterson, *Decision Analysis for the Manager* (New York: Holt, Rinehart & Winston, 1974); S. Barclay, R.V. Brown, C.W. Kelley, C.R. Peterson, L.D.Philips, and J. Selvidge, *Handbook for Decision Analysis* (McLean, VA: Decisions & Designs, Inc., September 1977); and Strategic Decision Group, *The Principles and Applications of Decision Analysis*, Ronald A. Howard and J.E. Matheson (eds.), 1983. Also see Rex V. Brown, "A Brief Review of Executive Agency Uses," op. cit.; and Rex V. Brown and Jacob W. Ulvila, "Selected Applications of Computer-Aided Decision Analysis and Support," OTA contractor report prepared by Decision Science Consortium, Inc., May 1985.

[22] See, for example, Michael F. Mitrione, "Integration of Decision Support Systems," *Military Review*, vol. 64, April 1983, pp. 52-59; Philip N. Sussman, "Evaluating Decision Support Software," *Datamation*, vol. 30, Oct. 15, 1984, pp. 171-172; Bernard C. Reimann and Allan D. Waren, "User-Oriented Criteria for the Selection of DSS Software," *Communications of the ACM*, vol. 28, No.2, February 1985, pp.166-179; and Allan F. Ayers, "Decision Support Systems—New Tool for Manufacturing," *Computerworld*, vol. 19, June 19, 1985, pp. 35-38.

[23] See, for example, Judith D. Bentkover, et al., *Benefits Assessment: The State-of-the-Art*, prepared by Arthur D. Little, Inc. for the National Science Foundation, December 1984; and Miley W. Merkhofer, et. al., *Risk Assessment and Risk Assessment Methods: The State-of-the-Art*, prepared by Charles River Associates, Inc. and Applied Decision Analysis, Inc. for the National Science Foundation, December 1984.

[24] See, for example, Kenneth L. Kraemer, "The Politics of Model Implementation," *Systems, Objectives, Solutions*, vol. 1, 1981, pp. 161-178; John Leslie King, "Successful Implementation of Large-Scale Decision Support Systems: Computerized Models in U.S. Economic Policy Making," *Systems, Objectives, Solutions*, vol. 3, 1983, pp. 183-205; John Leslie King, "Ideology and Use of Large-Scale Decision Support Systems in National Policymaking," *Systems, Objectives, and Solutions*, vol. 4, 1984; William H. Dutton and Kenneth L. Kraemer, *Modeling as Negotiating: The Political Dynamics of Computer Models in the Policy Process* (Norwood, NJ: Ablex, 1985); and Lance N. Antrim, "Computer Models as an Aid to Negotiation: The Experience in the Law of the Sea Conference," November 1984.

Further Testing and Development of the Decision Conference Technique

Despite the widespread and frequently sophisticated use of computer-based decision support by Federal agencies, the results of this effort appear to be used largely by agency staff or, at the most, presented to agency decisionmakers for consideration along with other inputs. There appear to be relatively few situations where the decisionmakers themselves actively participate in the decision analytic process. OTA located only one agency that has a formal program to do this—the decision conference facility of the Office of Program Planning and Evaluation in the Department of Commerce (DOC).

This DOC decision conference facility is used to bring key staff and decisionmakers together for, typically, 1 or 2 days to work through a real decision problem using whatever computer and analytical tools are appropriate. Decision conference staff do advance work prior to the conference and serve as facilitators, analytical experts, and rapporteurs during the conference. But the primary participants are the decisionmaker(s) and his or her staff. The DOC decision conferences use a wide range of computer-assisted analytical techniques—including spreadsheet software, quantitative, and qualitative judgmental—depending on what is most useful. The DOC facility is about 1 year old.[26] A list of illustrative decision conferences is shown in table 6-4.

OTA found that DOD does not appear to have such a facility, despite the very extensive DOD use of computer-based decision analytic techniques. DOD does have numerous de-

Table 6-4.—Illustrative Decision Conferences Conducted by the Office of Program Planning and Evaluation, U.S. Department of Commerce, 1984-85

1. Development of Program and Budget Priorities for the U.S. National Marine Fisheries Service: (a) FY 1986; (b) FY 1987.
2. Promotion of Tourism to the United States—An Assessment of Alternative Marketing Strategies Available to the Department of Commerce in Six Regional Foreign Markets.
3. Review of Alternative Programs and Service Delivery Strategies for the Minority Business Development Agency.
4. Allocation of Saltonstall/Kennedy Fisheries Development Grant Program Funds—Priority Setting for Grant Applications.
5. Assessment of Alternative Foreign Trade Strategies for Promoting the Export of Auto Parts to Japan.
6. Development and Evaluation of Alternative Staffing Standards for Selected, Governmentwide Administrative Functions (President's Council on Management Improvements): (a) Personnel; (b) Procurement; (c) Warehousing.
7. Assessment of Alternative Long-Term Goals, Strategies and Implementation Mechanisms for the Telecommunications, Computer, and Information Programs of the Department of Commerce.
8. Assessment of Alternative Long-Term Strategies for Promoting Technological Innovation and the Transfer of Technology from Federal Laboratories to the Private Sector (Preliminary).
9. Assessment of Alternative Operating Objectives and Resource Allocations for Selected Administrative Activities of the Department of Commerce: a) Personnel and Civil Rights Functions; b) Management and Information Systems Development; c) Financial Assistant Oversight Activities; and d) Regional Administrative Support Operations.
10. Alternative Programmatic Allocation of Field Personnel Resources, Center for Food Safety and Applied Nutrition of the U.S. Food and Drug Administration.

SOURCE: Office of Program Planning and Evaluation/Department of Commerce.

---

[25] See U.S. General Accounting Office, *Progress in Improving Program and Budget Information for Congressional Use*, GAO/PAD-82-47, Sept. 1, 1982; GAO, *The DOD Planning, Programming, and Budgeting System*, GAO/OACG-84-5, September 1983; GAO, *Cost-Benefit Analysis Can Be Useful in Assessing Environmental Regulations, Despite Limitations*, GAO-RCED-84-62, Apr. 6, 1984; GAO, *DOD Needs To Provide More Credible Weapon Systems Cost Estimates to Congress*, GAO/NSIAD-84-70, May 24, 1984.

[26] For more detailed discussion, see Charles Treat, "Commerce Computer Center Attracts Atttention," *Commerce People*, vol. 6, No. 4, April 1985, p. 5; Charles F. Treat, "Modeling and Decision Analysis for Management," a paper prepared for the Government Computer Expo, June 13, 1985; and William A. Maldens, "Better Data Doesn't Always Mean Better Decisions—Decision Analysis Does," *Government Executive*, November/December 1984, pp. 10, 14.

cision analytic support centers throughout the various service branches and commands, but they are at the staff and research levels. For example, the JCS staff conducts extensive studies (inhouse and by contract) using modeling and decision analytic techniques. But the Joint Chiefs themselves do not normally participate, except to the extent of approving the major studies. The results of selected decision analytic studies are presented to the Joint Chiefs when relevant to a decision problem at hand.

The decision conference appears to have substantial potential, but the general consensus among practitioners is that further development and testing are needed prior to widespread application. Moreover, at present few decisionmakers are even aware of the technique, and even fewer have tried it.

One of the keys to a successful decision conference is the direct and full participation of the decisionmakers. In order to have greater use of the technique, decisionmakers need both greater awareness and greater understanding of the technique. Conducting pilot tests in selected programmatic areas, holding a workshop or conference, and commissioning a special report on the subject are actions that could help improve awareness and understanding.

One of the areas thought to be most suited for the decision conference approach is R&D decisionmaking. The National Marine Fisheries Service (NMFS) (DOC) has already used a decision conference for decisions on the R&D budget for fiscal years 1986 and 1987. However, it should be noted that NMFS had been exploring decision analysis for several years, and thus appears to have been favorably predisposed.[27] Decision analytic studies also have been used as significant input to R&D decisions at DOD, although not in the decision conference format adopted at DOC.[28] At DOC, decision conferences have also been conducted on budget, programmatic, and strategic decisions.

The real power of the decision conference technique (or concept) is its potential to bring the full range of computer tools, models, analytical techniques, and the like into focus for the decisionmaker within a framework that is relevant to the decisionmaker. This is a concept that has been visualized and partially developed over the last 20 years or so by numerous researchers and innovators.[29] Table 6-5 places the decision conference in the context of other computer-supported conference room concepts. However, note that different decision conference configurations are possible. For example, DOC, in effect, uses software from the electronic boardroom and information center concepts *in addition to* the software listed under decision conference, and uses the orgware (i.e., organizational data and procedures) from the electronic boardroom and information center *instead of* the orgware listed under decision conference.

Overall, the decision conference concept is quite flexible, and many of the elements of the various concepts shown in table 6-5 are interchangeable. Thus it is perfectly feasible for a computer- or video-conferencing capability, for example, to be added to the decision conference. Indeed, OTA's Federal Agency Data Request revealed that some agencies are already using computer-conferencing, although not as part of decision conferences per se. For example, the U.S. Geological Survey (USGS) makes extensive use of computer-conferencing on such diverse topics as cartography, geoscience, computer hardware and software problems, USGS news releases, and Mount Saint Helens' volcanic activity bulletins.

---

[27] See Bruce Norman, "What Policy Analysis Can Do For You—A Survey," NMFS memo to Winfred H. Meibohm, Oct. 13, 1978; and Hoyt A. Wheeland, "NMFS Decision Analysis," NMFS memo to William H. Stevenson, June 16, 1982.

[28] For an illustration of R&D budgeting at the Defense Nuclear Agency, see J.W. Ulvila and J.O. Chinnis, Jr., "Analysis for R&D Resource Management," *Management of R&D and Engineering*, D.F. Kocaoglu (ed.) (North-Holland: 1985).

[29] Among the many researchers, the following are illustrative (in alphabetical order): Rex Brown, Dennis Buede, William Dutton, Kenneth Kraemer, John King, Starr Roxanne Hiltz, Lee Merkhofer, Thomas Sheridan, and Murray Turoff. For a good review and extensive references, see Kenneth L. Kraemer and John L. King, "Computer Supported Conference Rooms: Final Report of a State of the Art Study," December 1983, presented as a paper under the title "Computer-Based Systems for Group Decision Support" at the Academy of Management Annual Conference, Aug. 15, 1984.

Table 6-5.—Comparison of Computer-Supported Conference Room Concepts

Electronic boardroom:
Computer and audiovisuals

Information center:
Computer, databases, and software tools

Teleconferencing facility:
Computer and communications

Decision conference:
Computer and models

Element	Electronic boardroom	Teleconference facility	Information center	Decision conference
Hardware....	Conference room; audiovisuals; graphic displays; computer	Conference room; audiovisuals; audio, computer, or video telecommunication controller	Conference room; large-screen video projector; computer; display terminals	Conference room; large-screen video projector; display terminals; voting terminals
Software	Interactive graphics	Communications	Database management software; statistical packages; retrieval, graphics, and text processing software	Decision analysis software; modeling software; voting tally and display software
Orgware.....	Audiovisuals; corporate reports; standard meeting protocols	Audiovisuals; teleconference protocols	Corporate and other databases; standard meeting protocols, standard meetings (e.g., annual report, market forecast)	Democratic decisionmaking protocols (e.g., one person one vote; all major interests represented; majority opinion rules)
People	Participants; audiovisual technician	Participants (in two or more locations); teleconference facilitator	Participants; computer specialists; modeling specialists	Participants; decision analysts; group process facilitators
Examples ...	Not available. Custom-tailored for each site although some "modular" audiovisual rooms exist	Picturephone Meeting Service; Participate	HOBO System; SYSTEM W; EIS, Express, XSIM	Group Decision Aid; Decision Conferences of DDI and SUNY, Albany

SOURCE: Kenneth L. Kraemer and John L. King, "Computer-Supported Conference Rooms: Final Report of a State of the Art Study," December 1983, pp. 8-10.

Another variation on the decision conference concept is known as "interactive management," and is intended to deal with three principal functions of managers: 1) intelligence (finding and clarifying problems), 2) design (generating or conceptualizing new or improved alternative solutions), and 3) choice (selecting the preferred solution).[30] Like other decision conference concepts, the interactive management approach utilizes a "situation room" with appropriate audiovisual and computer support. What distinguishes interactive management is the explicit focus on intelligence, design, and choice, and the use of a specific set of methodologies to structure ideas, design alternatives, and analyze trade-offs.[31] Several Federal agencies have utilized the interactive management decision approach, including the Forest Service and Agricultural Research Service (Department of Agriculture); National Marine Fisheries Service (DOC); and Food and Drug Administration (Department of Health and Human Services).[32]

In sum, Kraemer and King's 1983 prognosis that computer-supported conference techniques are "likely to grow at a slow pace over the next 2 years, and pick up a bit thereafter"[33] may be coming true. It is now over 2 years later, and the decision conference technique (sometimes also known under the rubric of group decision support systems [GDSS] or strategic planning decision support systems [SPDSS]) is now considered to be at the cutting edge of computer-based decision analysis.[34]

---

[30] Alexander N. Christakis and David B. Keever, "An Overview of Interactive Management," Center for Interactive Management, George Mason University, Fairfax, VA, 1984.

[31] Ibid.

[32] See *CIM News*, fall 1985; and Alexander N. Christakis, "The National Forum on Nonindustrial Private Forest Lands," *Systems Research*, vol. 2, No. 3, pp. 189-199.

[33] Kraemer and King, "Conference Rooms," op. cit., p. 7.

[34] At the November 1985 meeting of ORSA/TIM, experts such as Warren Walker, Rand Corp.; Paul Gray, Clarement Graduate School; George Huber, University of Texas at Austin; and Shao-ju Lee, California State University at Northridge agreed on the need to develop and implement a GDSS or SPDSS concept as the state-of-the-art in DSS. Also see Bernard C. Reimann, "Decision Support Systems: Strategic Management Tools for the Eighties," *Business Horizons*, September-October 1985, pp. 71-77. Also see Fred B. Wood, "Prospects for General Systems Decision Support Centers in the Federal Government," paper prepared for the Annual Meeting of the Society for General Systems Research, Philadelphia, PA, May 1986.

DECISION SUPPORT AND GOVERNMENT FORESIGHT

Foresight can be properly viewed as part of decision support. In the context of the Federal Government, foresight typically refers to the ability of individual Federal agencies and the government collectively to monitor, anticipate, and analyze key longer term trends and their implications for public policy and programs. One objective of foresight is to help government decisionmakers better understand and consider longer term trends and implications when making decisions.

The major foresight sectors can be viewed as spanning the entire range of Federal Government programs and activities, including, for example: energy, environment, water, climate, food, population, transportation, housing, education, the economy, foreign trade, and national security. Not all techniques are equally applicable to all foresight sectors. Thus, for example, remote-sensing satellites are most applicable to the environmental and natural resources (e.g., including food, water, climate, land use) sectors of foresight. Large-scale modeling is most applicable to those sectors, such as energy and climate, where key variables and relationships can be quantified and where substantial input data are available. On the other hand, some decision analytic techniques (e.g., the decision conferences discussed earlier) are applicable to both quantitative and qualitative, observational and judgmental information, and thus are relevant to many, if not all, foresight sectors.

Information technology—including data collection, archiving, and transfer, as well as modeling and analytic techniques—now makes improved foresight possible. This potential is being facilitated by advances in:

- technical monitoring capability (e.g., through remote-sensing satellites, advanced data communication networks, and computerized data centers);
- computational and analytical capability (e.g., through the entire range of computer tools, from microcomputers to supercomputers, related software, and the procedures necessary for documenting and validating models); and
- the scientific and technical knowledge base in the wide range of disciplines that bear on foresight.

Realization of the potential for improved foresight appears to require: 1) a synthesis of technical advances that are here now or close at hand, 2) an integration of relevant information, and 3) institutional mechanisms that work across agency and disciplinary lines. Each of these is considered below.

Technical Advances

Relevant technical advances include microcomputers, supercomputers, remote-sensing systems, computerized databases, a wide range of software, and model evaluation procedures. Remote-sensing satellites and model evaluation are discussed here. Various applications of microcomputers, supercomputers, and related software were discussed under decision support. Techniques used to integrate information are discussed in a later section.

Remote Sensing

The advent of remote-sensing satellites has revolutionized the collection of data on many variables relevant especially to the natural resources and environmental aspects of foresight. Satellites provide far more extensive Earth coverage than could possibly be achieved through other means, especially for oceans and remote land areas. In addition, these satellites can receive, process, and retransmit data from radiosondes, ships, ocean buoys, and remote land-based automatic stations.

There are two basic types of environmental satellites: polar orbiting (or sun-synchronous) and geostationary (or geosynchronous). The polar orbiting satellites provide coverage of the entire Earth several times per day. The geostationary satellites cover only a portion of the Earth's surface, but coverage is continuous since the geostationary satellites maintain a constant orbital position relative to the Earth's surface. Illustrative kinds of data currently collected by remote-sensing satellites include:[35]

- cloud and snow mapping;
- volcanic eruptions and forest fires;
- urban sprawl;
- specific types of land cover (e.g., trees, crops, grassland);
- geologic fault lines;
- ice mapping (i.e., sea ice, mountain glaciers, ice sheets, ice shelves);
- changes in margins of glaciers (e.g., retreats and advances);
- surface temperature and weather (land and sea);
- cataclysmic weather events (e.g., hurricanes, severe storms);
- atmospheric and oceanic circulation patterns; and
- atmospheric temperature profiles and water content.

More advanced satellites are planned for the future, satellites that will observe all major aspects of the Earth system even more completely. As an illustration, NASA has developed the concept of the Earth-observing system, a future generation satellite that would build on learning from the current generation of operational satellites. Table 6-6 lists the types of parameters on which data would be collected and the types of applications. This list also represents the data needed for a unified approach to earth science, based, in NASA's words, "upon the view that the physical, chemical, and biological processes at work on Earth comprise a coupled global system."[36] Many of these parameters are relevant to foresight.

The volume of remote-sensing data relevant to foresight is truly staggering, especially when viewed on a global scale; and yet, the volume of data increases substantially every year, reflecting the high level of observational activity. The only answer to this data challenge is heavy use of computerized data centers and sophisticated data management, with data stored and disseminated in electronic form wherever possible. This is, indeed, the strategy followed over the last 10 years, to the point where the data archiving system now could not survive without information technology.[37]

Model Evaluation

Another example of a key technical advance important to foresight is model evaluation. Knowledge about how to improve computer modeling—through appropriate documentation, verification, and validation—could be systematically applied to at least the major models relevant to foresight.

Models are, by definition, abstractions of reality. For very complex systems, it is unlikely that a perfect model can or should be developed. A certain range of uncertainty is usually acceptable. However, to the extent decisionmakers use the results of models, they need to have confidence in the models. Confidence does not mean that the results are always 100 percent accurate. Confidence means that the decisionmaker (or other user) knows the strengths and limitations of the model, the applicability of the model for a particular decision, the sensitivity of the model to changes in key assumptions and in the model structure, and the range of uncertainty of model results.[38]

For large, complex models, such as many of those used in modeling relevant to foresight

---

[35] U.S. Department of Commerce, National Oceanic and Atmospheric Administration, National Environmental Satellite, Data, and Information Service, *NESDIS Programs: NOAA Satellite Operations*, March 1985, pp. 16, 70; also see section on Landsat, pp. 206-237.

[36] U.S. National Aeronautics and Space Administration, Goddard Space Flight Center, *Earth Observing System: Science and Mission Requirements Working Group Report*, vol. 2, August 1984, pp. 1, 9.

[37] For example, NOAA maintains three major computerized data centers that archive remote sensing (and many other kinds of) data: the National Climate Data Center in Asheville, NC; National Oceanographic Data Center in Washington, DC; and National Geophysical Data Center in Boulder, CO. All provide data variously in paper, microfiche, microfilm, photographic, computer tape, computer printout, and digital data form.

[38] Saul I. Gass and Lambert S. Joel, "Concepts of Model Confidence," *Computer and Operations Research*, vol. 8, No. 4, 1981, pp. 341-346.

Table 6-6.—Earth-Observing Data Parameters and Applications

Parameter	Application
Soil features:	
• Moisture	Hydrologic and geochemical cycles
—Surface	
—Root Zone	
• Types-areal extent (peat, wetlands)	Geochemical cycles Agricultural and forestry
• Texture-color	Agriculture and forestry
• Erosion	Geochemical cycles
• Elemental storage	Geochemical cycles
—Carbon	
—Nitrogen	
• Permafrost	Geochemical
Surface temperature:	
• Land	Primary production, soil moisture and respiration
• Inland waters	Mass/energy flux
• Ocean	Mass/energy flux
• Ice	Mass/energy flux
Vegetation:	
• Identification • Areal extent • Condition (stress, morphology, phytomass)	Hydrologic cycle, biomass distributions and change, primary production, plant productivity, respiration, nutrient cycling, trace gas, source sinks, vegetation-climate interaction, microclimate
• Leaf area index canopy structure and density	
Clouds:	
• Cover • Top height • Emission temperature • Albedo • Water content	Radiation balance, weather forecasting, hydrologic cycle, climatologic processes, tropospheric chemistry
Water vapor	Weather forecasting, hydrologic cycle, climatologic processes
Snow:	
• Areal extent	Hydrologic cycle
• Thickness	Water equivalent
Radiation:	
• Shortwave	Surface energy budget
• Longwave	Surface energy budget
• Short and long wave	Hydrologic cycle
Precipitation	Hydrologic cycle Climatologic cycle
Evapotranspiration	Hydrologic cycle
Runoff	Hydrologic cycle
Wetland areal extent	Hydrologic cycle Biogeochemical cycle
Phytoplankton:	Biogeochemical cycles
• Chlorophyll Open ocean/coastal Ocean/inland waters	
• Fluorescence Open ocean/coastal Ocean/inland waters	
• Pigment groups Open ocean/coastal Ocean/inland waters	
Turbidity:	Biogeochemical cycles erosion assessment
• Inland water/coastal ocean	
Bioluminescence	Ecological processes
Surface elevation:	
• Land	Continental tectonics and surface processes Interpretation and modeling of gravity and magnetic field data
• Ocean	Circulation
• Inland ice	Hydrologic cycle
Wave:	
• Height	Air-sea interactions
• Spectrum	
Inland ice:	
• Thickness	Ice dynamics
• Velocity field	Ice dynamics
• Mass balance temperature	Ice dynamics, hydrologic cycle, climate
Sea Ice:	
• Areal extent	Hydrologic cycle
• Concentration	Oceanic processes
• Sea ice dynamics	Climatological processes
Atmospheric constituents: (Ozone and compounds of carbon, nitrogen, hydrogen, chlorine, sulfur, etc.)	Tropospheric chemistry Middle atmosphere Upper atmosphere
Aerosols	Tropospheric chemistry Stratospheric chemistry
Temperature	Troposphere Middle atmosphere Upper atmosphere
Winds	Troposphere Middle atmosphere Upper atmosphere Surface
Lightning: (number of flashes, cloud to cloud, cloud to ground)	Tropospheric chemistry Atmospheric electricity
Emission features	Upper atmosphere
Electric fields	Global electric circuit
Rock unit minerology	Continental rock types Continental soil and rock types and distribution
Surface structure	Tectonic history
Gravity field	Mantle convection, oceanic lithosphere, continental lithosphere, sedimentary basins, passive margins, etc.
Surface stress	Weather forecasting, climate processes, oceanography
Oceanic geoid	Mantle convection, oceanic lithosphere
Magnetic field	Crust and upper mantle, composition and structure, lithospheric thermal structure, secular variation of main field (core problem), upper mantle conductivity
Plate motion	Plate tectonic theory, fault motion

SOURCE: NASA, *Earth Observing System*, August 1984, pp. 16-19.

(e.g., in energy, agriculture, climate, population, and transportation), developing a high degree of confidence is difficult. Frequently, the models are too complex to depend on guesswork or back-of-the-envelope evaluations. But a formal evaluation or assessment program costs time and money, and may be seen as a drain on resources needed for the modeling activity itself.

Nonetheless, there is now at least 10 years of work and research suggesting that a well-developed model evaluation program can help not only to increase decisionmaker (or user) confidence in the model, but also to actually facilitate the development of better models and better communication among modelers.[39] Such a program also could help overcome some of the problems that confronted the *Global 2000* study—inconsistent assumptions about key variables, omission of key variables, lack of clear model documentation, weak or inconsistent model validation, lack of analyses of model sensitivity to exogenous variables, omission of key feedback loops, and inconsistent input data.[40]

Because foresight by definition deals with the future, and because controlled global or hemispheric, or even national, experiments are rarely feasible, modeling is a critical tool of foresight. But even though the computer technologies and databases for modeling have improved substantially in recent years, most opportunities to improve the model evaluation process have not as yet been realized.

Prior research has reviewed many of the model evaluation frameworks proposed over the years. The results of a review conducted by Oak Ridge National Laboratory (ORNL) (DOE) found that evaluation elements could be grouped under the categories of model documentation, verification, validation, and usability. In reaching this finding, ORNL reviewed the work of the Massachusetts Institute of Technology (MIT) Energy Modeling Laboratory, Texas Energy Advisory Council, GAO, Professional Audit Review Team (mandated by Congress to review DOE's energy data collection and analysis, including models), Dr. Saul I. Gass (frequent consultant to NBS), and ORNL's own evaluation technology.[41]

Model evaluation is an activity that can be carried out by the modelers themselves, by model users, by model analysts or auditors, and/or by some combination. From the modeler's perspective, model evaluation is a natural component of the modeling process and may involve spontaneous peer review or more organized modeling groups, meetings, and workshops. On a more formal basis, model evaluation may involve modeling standards or guidelines, formal user reviews or consultant studies, modeling laboratories, and outside audits.[42] An MIT approach to evaluation of energy models is shown in figure 6-1, and could have general applicability to foresight-related models.[43]

Aspects of the evaluation process for DOE's energy models were discussed previously (see table 6-3 and related text). DOE has also funded an evaluation of the major climate models (primarily large-scale general circulation models run on supercomputers) used to

---

[39] See U.S. General Accounting Office, *Ways To Improve Management of Federally Funded Computerized Models*, Aug. 23, 1976; *Models and Their Role in GAO*, October 1978; *Guidelines for Model Evaluation*, January 1979; U.S. Department of Commerce, National Bureau of Standards, *Utility and Use of Large-Scale Mathematical Models*, Saul I. Gass (ed.), May 1979; *Validation and Assessment of Energy Models*, Saul I. Gass (ed.), October 1981; Also see U.S. Congress, Office of Technology Assessment, *Use of Models for Water Resources Management, Planning, and Policy*, OTA-O-159 (Washington, DC: U.S. Government Printing Office, August 1982). Also see U.S. Council on Environmental Quality and U.S. Department of State, *The Global 2000 Report to the President: The Technical Report—Volume Two* (Washington, DC: U.S. Government Printing Office, 1980); U.S. Congress, Office of Technology Assessment, *Global Models, World Futures, and Public Policy* (Washington, DC: U.S. Government Printing Office, April 1982); and Donella Meadows, John Richardson, and Gerhart Bruckman, *Groping in the Dark: The First Decade of Global Modeling* (New York: John Wiley & Sons, 1982).

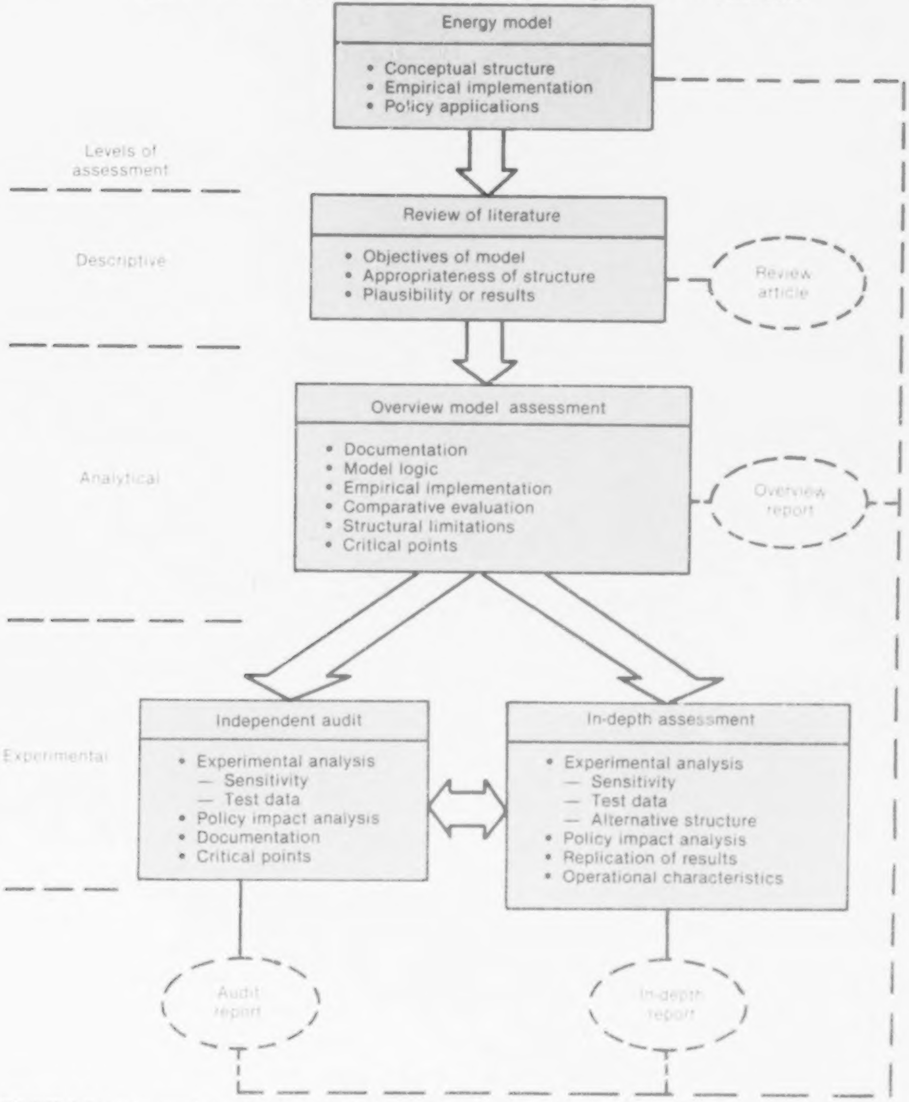
[40] *Global 2000*, ibid., esp. ch.14, pp. 453-499.

[41] C.R. Weisbein, R.W. Peele, and A.S. Loebl, "An Approach To Evaluating Energy-Economy Models," *Energy*, vol. 6, No. 10, 1981, pp. 999-1027.

[42] Martin Greenberger and Richard Richels, "Assessing Energy Policy Models: Current State and Future Directions," *Annual Review of Energy*, vol. 4, 1979, pp. 467-500.

[43] See D.T. Kresge, "An Approach to Independent Model Assessment," *Validation and Assessment Issues of Energy Models Workshop*, National Bureau of Standards, NBS SP 569, 1980.

Figure 6-1.—An Approach to Evaluating Energy (and Other) Models


Energy model
• Conceptual structure
• Empirical implementation
• Policy applications
Levels of assessment
Review of literature
Descriptive
• Objectives of model
• Appropriateness of structure
• Plausibility or results
Review article
Overview model assessment
Analytical
• Documentation
• Model logic
• Empirical implementation
• Comparative evaluation
• Structural limitations
• Critical points
Overview report
Independent audit
Experimental
• Experimental analysis
— Sensitivity
— Test data
• Policy impact analysis
• Documentation
• Critical points
In-depth assessment
• Experimental analysis
— Sensitivity
— Test data
— Alternative structure
• Policy impact analysis
• Replication of results
• Operational characteristics
Audit report
In-depth report

SOURCE: D.T. Kresge, reprinted in C.R. Weisbin, R.W. Peelle, and A.S. Loebl, "An Approach To Evaluating Energy Economy Models," Energy, vol. 6, No. 10, 1981.

simulate the effects of increasing atmospheric carbon dioxide.

The results of this evaluation illustrate several general points that appear to be applicable to most or all foresight-related models:

- there are many ways in which model results can be interpreted or misinterpreted;
- even the large, relatively well funded and heavily researched models are likely to have significant limitations in model variables, structure, and data;
- direct comparison of model variables, structure, and input data can help improve understanding of similarities and differences, strengths and weaknesses of model results;
- a model evaluation process can facilitate communication among researchers, especially where the models involve several different disciplines (which is typically the case with foresight-related models); and
- model evaluation techniques are sufficiently mature for application to even the most complex models.

Thus, by way of illustration, Professor Michael E. Schlesinger of Oregon State University, who conducted the recently completed DOE evaluation, found that:

> . . . the [climate] models might agree extensively in their simulated CO$_2$-induced climatic changes and yet be all wrong, and the models might simulate the present climate perfectly and yet be wrong in their simulated CO$_2$-induced climatic change.[44]

Dr. Schlesinger concluded that, although the latest general circulation model results show considerable agreement with respect to simulated global mean surface temperature change, there are substantial disagreements as to the geographical distribution of these changes. The differences in model results and the known model weaknesses (including use of questionable assumptions about key variables) mean that "not all of these simulations can be correct, but all could be wrong."[45]

Comparison of the structures and assumptions of the various climate models has shown some significant differences. While the major climate modeling centers continually work to improve their models, a formal program of model intercomparison and sensitivity studies is only just beginning. In 1984, an intercomparison was conducted of the ways in which radiative processes are incorporated into general circulation models.[46] The participants reportedly found this to be a very useful activity, which could be extended to other key areas of uncertainty, such as clouds, ocean coupling, sea ice, surface albedos (including snow, ice, land, vegetation), transient (as opposed to steady state) response, and atmospheric turbidity (e.g., from volcanic eruptions and air pollution).[47]

This approach appears to have potential for all foresight-related models, regardless of the focus of modeling, whether it be energy, environment, food, population, climate, or international trade. A key evaluation question is whether there are plausible changes in model processes and variables and/or the addition of new processes and variables that could substantially affect the model results, and also whether the range of uncertainty is small enough such that significant effects are highly probable under any plausible scenario.

Relevant Information

In addition to the technologies illustrated above (remote sensing and model evaluation) and those discussed previously, improved foresight requires relevant information presented in an integrated format. Information needs to be relevant and integrated in order to focus on those trends and relationships that are critical to the major foresight sectors (e.g., food, water, energy, climate, housing, population, environment, employment, economic development, and transportation) and the important relationships between sectors.

---

[44] Michael E. Schlesinger, Oregon State University, letter to Fred B. Wood of OTA, Aug. 28, 1985.

[45] See Michael E. Schlesinger and John F.B. Mitchell, "Model Projections of Equilibrium Climatic Response to Increase CO$_2$ Concentration," U.S. Department of Energy state-of-the-art paper, in press; also see Michael E. Schlesinger, "Atmospheric General Circulation Model Simulations of the Modern Antarctic Climate," *Environment of West Antarctica: Potential CO$_2$-Induced Change*, Polar Research Board, National Research Council (Washington, DC: National Academy Press, 1984), pp. 155-196.

[46] See F.M. Luther, *The Intercomparison of Radiation Codes in Climatic Models (ICRCCM): Longwave Clear-Sky Calculations*, WCP-93, World Climate Programme, 1984; also see U.S. Department of Energy, Carbon Dioxide Information Center, "Radiation Codes in Climate Models—A Comparative Study," *CDIC Communications*, spring 1985, p. 1.

[47] R.E. Dickinson, "How Will Climate Change: The Climate System and Modelling of Future Climate," ch. 5, B. Bolin (ed.) (Chichester, West Sussex: John Wiley & Sons, Ltd., in press).

In the Federal Government, sources of relevant information include all cabinet departments and many independent agencies. For example, the *Global 2000* study was based largely on data and analyses from the U.S. Departments of Agriculture; Commerce (Bureau of the Census, National Oceanic and Atmospheric Administration); Energy (EIA, Brookhaven National Laboratory); Interior (including USGS, Bureau of Mines); and State (including the Agency for International Development), the Environmental Protection Agency, and some outside groups (e.g., the World Bank for world gross national product projections).[48] The *Global 2000* study would not have been possible without the already existing activities relevant to government foresight of key trends. Likewise, the Joint Chiefs of Staff global "Forecast" model (discussed later) is dependent on a wide range of national and international data sources.

The results of the OTA Federal Agency Data Request used in this study indicate that all cabinet level agencies and many independent agencies use some computer models and maintain some databases that appear, at least on paper, to be relevant to foresight, although such activities are rarely, if ever, explicitly labeled "foresight."[49] In addition, many agencies are quite active in the international arena with numerous bilateral agreements and treaties that frequently provide for the exchange of information—information that is likely to be relevant to government foresight. The subject areas of such agreements and treaties span the spectrum from agriculture, earth sciences, and oceanography to forestry, water, climatology, and environment.[50] There are also numerous nongovernmental sources of foresight information.

A major foresight challenge is sorting out the information most important to monitoring and analyzing key trends and their implications. Three relatively recent developments have made this somewhat easier:

1. the maturation of systems science for analysis of complex trends and issues relevant to foresight;
2. the availability of data integration and graphics display equipment that can present and manipulate multiple databases quickly and concisely; and
3. the maturation of analytical and decision support techniques that can help synthesize both quantitative and qualitative information—including ranges of uncertainty—into a format that is usable by decisionmakers.

Systems Science

Numerous systems researchers—such as Ludwig von Bertallanfy, Karl Deutsch, Stafford Beer, Ervin Laszlo, Geoffrey Vickers, and Richard Ericson—have articulated the potential of systems and cybernetics (communications and control) concepts to improve the decisionmaking processes and "steering" mechanisms of government.[51] A common goal has been to design a system (or systems) that brings key information to the attention of decisionmakers, and helps structure and analyze that information so as to facilitate better understanding of the complexities and interrelationships among significant variables.

---

[48] *Global 2000, Volume Two*, op. cit., pp. 484-499.

[49] See illustrations of computer modeling and decision support presented earlier in this chapter; also see ch. 7 discussion and illustrations of agency databases.

[50] U.S. Department of State, "U.S. Government Participation in International Treaties, Agreements, Organizations, and Programs in the Fields of Environment, Natural Resources, and Population," an inventory prepared at the request of the Federal Interagency Global Issues Work Group, January 1984, pp. B-1 to B-12 and pp. E-2 to E-6.

[51] See, for example, Ludwig von Bertallanfy, *General Systems Theory: Foundations, Development, Applications* (New York: Braziller, 1968); Karl W. Deutsch, *The Nerves of Government: Models of Political Communication and Control* (New York: MacMillan/Free Press, 1963); Stafford Beer, *Decision and Control: The Meaning of Operational Research and Management Cybernetics* (New York: Wiley, 1966); Ervin Laszlo, *A Strategy for the Future* (New York: Braziller); Geoffrey Vickers, *Making Institutions Work* (New York: Wiley, 1973); and Richard F. Ericson, "Thinking and Management Values in the Microchip Era: An Action Agenda for Institutional Transformation," *Systems Research* 2 (vol. 1), 1985, pp. 29-32.

Systems science is applicable to all foresight sectors, and especially those that are characterized by complex feedbacks and interactions among variables or components. For example, in 1982, James G. Miller wrote that:

> Subsystems of the Earth system consist of sets of interacting components, each such set concerned with particular processes. Because of interactions, including feedbacks among subsystems, changes in one part of the system may have effects throughout the whole system.[52]

Indeed, research results from specific disciplines (e.g., in such fields as geology, oceanography, glaciology, atmospheric sciences, and paleoclimatology) are being published at a rapid rate and are shedding new light on various aspects of the Earth system. These research directions appear to be converging on the need to better monitor and understand the Earth as an interactive system involving the atmosphere, oceans, glacial and volcanic cycles, land mass, and biota (plants, forests, animals, etc.).[53] The Earth systems approach can serve as an important foresight methodology.

The significance of this convergence of technology (e.g., remote sensing and computers) with the scientific research enterprise is now well recognized, and cited as one of the rationales for such new initiatives as the Global Habitability Program and International Geosphere-Biosphere Program.[54] In the words of NASA's Dr. Burton I. Edelson, in a *Science* editorial:[55]

> Modern technology has given us the tools of measurement and of computation to study the earth as a system. We can now gain comprehensive knowledge, not only of the state of the earth system and of global processes, but also of changes in state and processes. We have become uncomfortably aware that changes are indeed taking place, and we know that our own species is responsible for some of the changes.

Data Integration and Display

Fortunately, computer graphics and data management equipment that can integrate and display large amounts of data are now available. There are many products under development or on the market. As one example, NASA has developed a comprehensive data management and analysis system, known as the Pilot Climate Data System (a related version is called the Pilot Ocean Data System), that has broad applicability to a wide range of variables relevant to foresight and could serve as a key component of a state-of-the-art "global foresight data display."[56] While the pilot system includes primarily atmospheric and oceanographic databases, the system concept could be easily extended to cover other foresight-related databases.

The system is run on a mainframe computer with user-friendly, menu-driven software. The system has an on-line catalog of all available data, an on-line inventory of data sets available, a data manipulation subsystem (including the capability for statistical evaluation and merging, averaging, etc., of data sets), and a state-of-the-art graphics subsystem (including two- and three-dimensional color).

Another example is the Decision Information Display System (also developed with NASA support) that was designed to integrate and display selected domestic and international data, statistics, and trends in a geographic format. This system has been used on occasion by some staff of both the Carter and Reagan White Houses.[57] This system also

---

[52] James Grier Miller and Jessie L. Miller, "The Earth as a System," *Behavioral Science*, October 1982, p. 310. Also see J.E. Lovelock, *GAIA: A New Look at Life on Earth* (Oxford: Oxford University Press, 1979).

[53] See, for example, Norman Myers, *GAIA: An Atlas of Planet Management*, (Garden City, NY: Anchor Books, 1984); Owen B. Toon and Steve Olson, "The Warm Earth," *Science 85*, October 1985, pp. 50-57.

[54] M. Mitchell Waldrop, "An Inquiry Into the State of the Earth: Technology Is Making It Possible To Study the Earth as an Integrated System; Problems Like Ozone and Acid Rain are Making It Imperative," *Science*, Oct. 5, 1984, pp. 33-35.

[55] Burton I. Edelson, "Mission to Planet Earth" (editorial), *Science*, Jan. 25, 1985.

[56] National Aeronautics and Space Administration, *Pilot Climate Data System*, undated brochure, pp. 1-8.

[57] Ronald H. Hinckley, "Information Systems for Elite Decision-making: The White House," paper presented at the 1985

(continued on next page)

could be extended to include a broad range of foresight-related data, statistics, and trends.

A further illustration is the Crisis Management Center (CMC) operated by the White House National Security Council. CMC includes a conference room with state-of-the-art audiovisual and graphics technology, multidimensional charts, and the capability to quickly convert textual material into statistical tables and graphics.[58] Robert C. McFarlane, former National Security Advisor to the President, described CMC as providing staff support for crisis decisionmaking:

> The center conducts pre-crisis collection and analysis of information about likely areas in an effort to anticipate events and to provide extensive background to decisionmakers as a crisis preventive. The center also provides analytical capabilities that can be drawn upon during a crisis. . .[59]

A final example is the "Forecasts" global model developed for the Joint Chiefs of Staff in DOD. "Forecasts" is basically an outgrowth of previous global modeling efforts, especially the World Integrated Model and Global Macro-Dynamic Model, and was recently updated at a cost of about $1.2 million. The model integrates trend data in key areas, such as agriculture (e.g., yield, land under cultivation, exports, imports for various crops), soils (arable, non-arable), water resources (surface, ground), energy sources (e.g., fossil fuel, hydro, wood), population, transportation, and the domestic economy. The model includes the following major sectors and categories:[60]

- geographic characteristics (e.g., land area, access to sea, and infrastructure such as roads, rail lines, airports, and waterways);
- natural resources (e.g., strategic non-fuel, fuel minerals, other energy sources, soils, and water resources);
- human resources (e.g., population by sex and urban v. rural birth, death, and growth rates, literacy, and median income);
- human resources (e.g., population by sex and urban v. rural, birth, death, and growth rates, literacy, and median income);
- human services (e.g., health, medical care, nutrition, housing, education, and social programs);
- industrial (e.g., agriculture, including grains, non-grains, industrial crops, livestock, and fish; manufacturing, including durable and non-durable goods, electric power, communication, and construction);
- economic variables (e.g., gross national product, balance of payments, and allocation of government expenditures);
- political attributes (e.g., type of government, philosophy, stability, and political parties); and

The data are aggregated by country and region, and the model is capable of monitoring key trends and forecasting these trends based on trend extrapolation and relatively simple relationships between variables. The model does not include all important variables and does not incorporate many important dynamics. For example, the model excludes most climatic trends (the exceptions being mean annual temperature and precipitation) and climate dynamics.[61] Thus, the model is quite limited in its ability to relate climatic changes and trends to, for example, trends in energy consumption, arable land acreage, global food markets, and the incidence of famine. Nonetheless, "Forecasts" is one of the most complete (and probably among the most heavily funded) approaches to integrating foresight information in the Federal Government.

All of these approaches could have a useful role in government foresight across the board, not just in NASA research laboratories, the

---

(continued from previous page)

Annual Meeting of the American Political Science Association, New Orleans, pp. 7, 9; also see Edward K. Zimmerman, "The Evolution of the Domestic Information Display System: Toward a Government Public Information Network," *Review of Public Data Use*, June 1980, pp. 69-81; and Richard S. Beal, "The Transformation to Informatics," a plenary address presented at the May 1981 National Computer Conference, Chicago.

[58] Hinckley, "Information Systems," op. cit., p. 12.

[59] Ibid., pp. 11-12; also see Robert C. McFarlane, Richard Saunders, and Thomas C. Shull, "The National Security Council: Organization for Policy Making," *The Presidency and National Security Policy*, Gordon R. Hoxie (ed.)(New York: Center for the Study of the Presidency, 1984), pp. 261-273.

[60] See U.S. Department of Defense, Joint Chiefs of Staff, "Forecasts Overview," undated; and Patricia G. Strauch, "The FORECASTS System—U.S. Global Model," *Futures*, October 1984, pp. 564-566.

[61] Joint Chiefs of Staff, "Forecasts," op. cit.

White House, or Joint Chiefs of Staff. However, these approaches still fall short of the fully integrative capability needed in foresight and, more generally, high-level decisionmaking, of which foresight is a key component.

Advanced Decision Support Techniques

Electronic databases, computer models, and the like are helpful and necessary, but not sufficient by themselves for high-level decision support and foresight. The central functions of foresight (and decision support generally) are to:

1. help decisionmakers integrate information relevant to decisions at hand;
2. broaden the perspective and improve the understanding of decisionmakers vis-a-vis the direct and indirect factors that may affect or be affected by a decision; and
3. alert decisionmakers to the strengths, weaknesses, risks, and uncertainties in the information and analyses relevant to a particular problem or decision area.[62]

This is obviously a difficult challenge, and one that, in the opinion of many who have served or conducted research in top-level government policy offices, has not received adequate attention. For example, Dr. Ronald Hinckley, a political scientist who has served on the National Security Council Staff, has concluded that:[63]

> The decisionmaking process in the White House is driven by an incomplete information support system. There is an abundance of information transfer (communications) technology, a heavy emphasis on information management (office automation) technology, but insufficient information integration (synthesis and conceptualization) technology. . . The dilemma is that while the President simply cannot have enough information, he and his top advisors often get too much of it because of lack of integration.

Another White House staffer has described the information integration problem in these terms:[64]

> We spend billions and billions of dollars to collect information to get it from the field to an analyst in the bowels of the bureaucracy. . . But having spent a lot of money to sustain an information collection, dissemination, and analysis process, we spend virtually nothing on direct support to a senior-level policymaker. . . We have very few analytic tools for the very high-level people.

In the view of Dr. Hinckley:

> . . . [t]he answer is probably not significantly more computing power; we basically have enough to bring our knowledge base up to par with the technological base.[65]

Part of the answer to improving foresight and decisionmaking may be the decision conference concept. Of all the decision analytic techniques reviewed earlier in this chapter, the decision conference concept stands out because of its potential to integrate data, information, and analyses relevant to a specific decision or problem in a context that is relevant to the decisionmaker(s) and with the full participation of both the decisionmaker(s) and staff (experts, analysts, etc.). In contrast, most decision analytic techniques and computer models are used by individual or groups of analysts, researchers, and scientists, and usually only the results, if anything, ever reach the decisionmaker. Even then, results typically must permeate several institutional layers. The decisionmakers are not actively engaged in the use of decision analytic tools and models.

The decision conference technique is intended to help the decisionmaker make better, more informed decisions and to make those decisions with better foresight. As discussed previously, DOC is the only Federal agency known to have a decision conference facility. The director of that facility reports favorable results from the relatively few decision conferences conducted to date, but no formal evaluations have been conducted. The basic idea is to help the decisionmaker and his or her staff work through a decision problem in a reasonably structured way so that options and implications can be clearly identified and evaluated using the best available information. The information can be drawn from a wide variety of sources—prior studies, results of computer modeling, expert opinion, decisionmaker opinion, key trends, and the like. Decision analytic and presentational tools (e.g., computer software and graphics) can be applied on the spot, for example, to help structure and evaluate options.[66] A few Federal agencies have also tried the decision conference approach known as "interactive management." The director of the Center for Interactive Management at George Mason University also reports favorable results.[67]

---

[62] See, for example, Lindsey Grant, *Thinking Ahead: Foresight in the Political Process* (Washington, DC: The Environmental Fund, 1983); and Joseph F. Coates, "Foresight in Federal Government Policymaking," *Futures Research Quarterly*, summer 1985, pp. 29-53.

[63] Hinckley, "Information Systems," op. cit., p. 7.

[64] Richard S. Beal, National Security Council official, quoted in Hinckley, ibid., p. 6.

[65] Ibid., p. 15.

Possible limitations on the decision conference techniques include the usual requirement that the decisionmakers participate in the entire decision conference—frequently lasting up to 2 days or more, a major time commitment for most decisionmakers. But perhaps the major limitations are lack of: 1) understanding of the technique; 2) recognition and acceptance of a need for the technique (or perhaps any so-called decision aids); and 3) desire to make decisions in a relatively visible, participative way. Some of these limitations can probably be overcome through education and training and the cumulative results of successful decision conferences.

In any event, the technique seems worthy of experimentation and relevant to foresight —given the inherently complex, multivariate, and uncertain trends and issues that foresight must address. An important point is that policymakers usually do not need, nor do they expect, perfect information. Waiting for perfect information very often means waiting until it is too late to make a decision, or too late to do anything about the problem even if a decision is made. For example, in the case of climate, some researchers believe that ocean thermal lag is masking the effects of increasing atmospheric carbon dioxide so that by the time a clear signal is detected, further and possibly substantial climatic change will be inevitable. Of course, other researchers believe that scientific uncertainty over the climatic effects of rising carbon dioxide levels is such that no clear conclusions can yet be drawn.[68]

One or several decision conferences could be held on a pilot basis—with the participation of scientists, policy analysts, and interested decisionmakers—to test the technique in selected foresight sectors, such as energy, agriculture, and climate. The pilot tests could focus on, for example, whether uncertainties and sensitivities in key trends and forecasts are low enough to warrant serious consideration of specific policy options; what the range and magnitude of effects of the options might be; and whether, and in what areas, additional research needs to be conducted. The decision conference(s) could explicitly test the sensitivities of policy options and effects to a wide range of trends and forecasts, including not only those generated by major modeling and research centers, but also those from smaller research centers, independent researchers, and international researchers.[69]

---

[66] See Charles Treat, "Commerce Computer Center Attracts Attention," *Commerce People*, vol. 6, No. 4, April 1985, p. 5; Charles F. Treat, "Modeling and Decision Analysis for Management," a paper prepared for the Government Computer Expo, June 13, 1985.

[67] The current director of the Center for Interactive Management at George Mason University is Alexander N. Christakis.

[68] For discussion of ocean thermal lag, see James E. Hansen, et. al., "Climate Sensitivity: Analysis of Feedback Mechanisms," *Climate Processes and Climate Sensitivity*, J.E. Hansen and T. Takahashi (eds.) (Washington, DC: American Geophysical Union, 1984), pp. 130-163, esp. p. 33; and Michael E. Schlesinger, W. Lawrence Gates, and Young-June Han, *The Role of the Ocean in CO_2-Induced Climate Change: Preliminary Results From the OSU Coupled Atmosphere-Ocean General Circulation Model*, report No. 60, Climatic Research Institute, Oregon State University, January 1985, pp. 31-34 published in J.C.J. Nihoul (ed.), *Coupled Ocean-Atmosphere Models* (Amsterdam: Elsevier, 1985). For discussion of other scientific views and uncertainties, see, for example, Richard C.J. Somerville and Lorraine A. Reimer, "Cloud Optical Thickness Feedbacks in the CO_2 Climate Problem," *Journal of Geophysical Research*, vol. 89, No. D6, Oct. 20, 1984, pp. 9668-9672; J. Oerlmans, "Response of the Antarctic Ice Sheet to a Climatic Warning: A Model Study," *Journal of Climatology*, vol. 2, 1982, pp. 1-11; Hugh W. Ellsaesser, "The Climatic Effect of CO_2: A Different View," *Atmospheric Environment*, vol. 18, No. 2, 1984, pp. 431-434; and Sherwood B. Idso, "Do Increases in Atmospheric CO_2 Have a Cooling Effect on Surface Air Temperature," *Climatological Bulletin*, October 1983, pp. 22-25.

Institutional Mechanisms

The third ingredient needed to improve the government's foresight capability, in addition to the technical, informational, and analytical advances discussed above, is a supportive institutional framework. This is a difficult challenge because foresight, by definition, cuts across agency and disciplinary lines. The primary foresight sectors collectively involve virtually every cabinet-level department of the U.S. Government and many of the independent agencies. Several of the foresight sectors singly involve multiple departments and agencies. For example, energy foresight, taken alone without considering impacts on and relationships with other foresight sectors, involves departments such as Energy, Interior, and Agriculture. Water foresight involves the Interior, Agriculture, and Commerce Departments, among others. And climate foresight involves the Commerce, Energy, and Defense Departments, along with NASA and NSF among others.

Based on the results of the OTA Federal Agency Data Request, OTA workshops on related topics, and interviews with numerous Federal agency officials, it seems clear that decision support and foresight functions operate with minimum to no coordination and integration at the agency level and governmentwide. Computer modeling, decision support, and foresight generally are not viewed as part of information technology management within the agencies or at OMB and GSA. Likewise, decision analytic and foresight information usually is not easily accessible from agencies or governmentwide.

Thus, an improved government foresight capability appears to require more effective institutional mechanisms at both the agency-specific and governmentwide levels with respect to coordination of foresight activities and exchange of and access to foresight information.

Agency-Specific

One alternative is to define foresight as being within the formal definition of the information resources management (IRM) concept and the responsibility of each agency's IRM officer. Right now, IRM does not include foresight, even though foresight is clearly an information function and heavily dependent on the use of information technology. The Paperwork Reduction Act is silent on foresight per se, although the act could be interpreted to extend to all Federal agency information activities and all agency use of information technology.

The Office of Management and Budget (OMB) could require that consideration of foresight capabilities and activities be included in each agency's IRM plan and in the governmentwide 5-year IRM plan, which is updated annually. The General Services Administration could provide guidance to agencies on how to incorporate foresight capability as part of the triennial IRM review process. (See chs. 2 and 3 for further discussion of the IRM planning and review process.) These changes could also be encouraged or directed by Congress through legislative amendments (e.g., to the Paperwork Reduction Act) and/or reports, accompanying the appropriate authorizing and appropriations acts for specific agencies and/or OMB.

---

[69] For climate and energy foresight analyses, one illustrative approach might be to start with a broad range of policy options such as those in Thomas C. Schelling, "Climatic Change: Implications for Welfare and Policy," in National Academy of Sciences, *Changing Climate*, op. cit., pp. 449-482, or, for energy options, see David J. Rose, Marvin M. Miller, and Carson Agnew, "Reducing the Problem of Global Warming," *Technology Review*, May/June 1984, pp. 49-58. The sensitivity of the options to widely varying trends and forecasts could then be examined, ranging from the results of the major U.S. climate models (see, for example, Schlesinger and Mitchell, "Model Projections," op. cit.), to simple extrapolations of current trends, to alternative hypotheses such as those developed by John Hamaker, *Survival of Civilization*, (Lansing, MI: Hamaker-Weaver Publishers, 1982) and Kenneth E.F. Watt "An Alternative Explanation of Widespread Tree Mortality in Europe and North America," April 1985, in preparation, to the results, if available, of U.S.S.R. research and modeling efforts (see, for example, A. Ryabchikov, *The Changing Face of the Earth: The Structure and Dynamics of the Geosphere, Its Natural Development and the Changes Caused by Man* (Moscow: Progress Publishers, 1975), and N.N. Moiseev, V.V. Aleksandrov, et.al., "Global Models, the Biosphere Approach (Theory of the Noosphere)," International Institute for Applied Systems Analysis, Laxenburg, Austria, July 1983)).

Another alternative is to include foresight formally as part of decision support, and encourage or direct agencies to establish a decision support center, if they do not already have one. These centers could be responsible for each agency's role in implementing any governmentwide foresight initiatives. The key point is to establish a focus of responsibility for foresight within each agency, such as the agency IRM officer or the agency decision support center or office.

A final alternative that complements the above is to include foresight and decision support in any enhanced information technology innovation program that may be established. Should one or more innovation centers be created, the center could provide information and assistance to individual agencies on implementing their own decision support and foresight centers.

Governmentwide

For at least the last 35 years, proposals have been made to set up some kind of governmentwide foresight office or the equivalent. For example, many of the study commissions established over the years, from the 1951 Materials Policy Commission to the 1976 National Commission on Supplies and Shortages, have recommended:

> . . . the establishment of a permanent body somewhere high in the executive branch for performing continuous futures research and analysis.[70]

In addition, the 1980 *Global 2000* study concluded that establishment of an ongoing institutional mechanism in the executive branch was essential to improve the government's long-term global analytic capabilities. *Global 2000* identified numerous problems with the computer models that formed the basis for the analysis, as discussed earlier. *Global 2000* envisioned an ongoing institutional entity with a major role in addressing these problems and, in general, improving the understanding of models and the quality and consistency of the analytic structures and databases on which the models depend.[71]

At present, while there is no governmentwide foresight office, the Council on Environmental Quality in the Executive Office of the President (EOP) coordinates an interagency Global Issues Working Group. The group meets infrequently, with a very limited staff and agenda. Nonetheless, it has sponsored the preparation of several useful documents prepared by agency staff and/or consultants.[72]

In the legislative branch, several key milestones establishing the congressional role in government foresight include:[73]

- enactment of the Technology Assessment Act of 1972, which created the Office of Technology Assessment;
- amendment of House Rule X, Section 101(b)(1) in 1974 to require each standing committee of the House of Representatives, except Appropriations and Budget, to include in their oversight duties "futures research and forecasting on matters within the jurisdiction of that committee";
- authorization of the Congressional Research Service (CRS) to create a Futures Research Group;
- creation of the Congressional Clearinghouse on the Future in 1975; and
- amendment of Rule 29 of the Standing Rules of the Senate in 1977 to require each Senate Committee, except Appropriations, to prepare a report on the future regulatory impact of proposed legislation.

Implementation of these actions has been mixed. For example, the CRS Futures Research Group has been disbanded as a separate entity, but its functions have been dispersed to other CRS divisions—principally the Government Division and the Science Policy Research Division. Relatively few House committees have conducted foresight hearings under House Rule X, but those few have compiled quite a substantial body of useful information. Two of the most active House committees with respect to foresight—the Committee on Energy and Commerce and the Committee on Science and Technology—issued at least six reports on foresight topics between May 1976 and April 1983.[74] Finally, although OTA does not generally issue foresight reports per se, foresight on advances in science and technology and their implications are incorporated into many OTA studies and reports.

---

[70] *Global 2000, Volume Two*, op. cit., p. 710.

[71] Ibid., pp. 460-484.

[72] See testimony of A. Alan Hill, Chairman, Council on Environmental Quality, Executive Office of the President, before the Apr. 30, 1985, joint hearing on "Global Forecasting Capability of the Federal Government," conducted by the Subcommittee on Government Efficiency of the Committee on Governmental Affairs and the Committee on Environment and Public Works, U.S. Senate.

[73] U.S. Congress, House of Representatives, Committee on Energy and Commerce, *Congressional Foresight: History, Recent Experiences, and Implementation Strategies*, a report prepared by the Congressional Research Service, 97th Cong., 2d sess., December 1982, pp. 3-4.

The current debate focuses in part on what kind of new or revised executive branch mechanisms are needed to facilitate government foresight, on the assumption that most foresight activities occur in the agencies and that coordination of these activities must come primarily from the executive branch of government.

The basic alternatives, other than doing nothing, involve strengthening the foresight functions of an existing office (or offices) or establishing a new office. While a governmentwide foresight office could, in theory, be located in any department or agency, most proposals suggest a location in the EOP, on the grounds that cabinet departments are much more likely to cooperate with an EOP entity. Several existing EOP offices are potential candidates for stronger foresight responsibilities—the Council on Environmental Quality, OMB, the Office of Science and Technology Policy, and possibly the Council of Economic Advisors.

Legislation to establish a more formalized governmentwide foresight function has been proposed on several occasions. Most recently, in April 1985, the "Critical Trends Assessment Act" (S. 1031) was introduced to establish an Office of Critical Trends Analysis in the EOP, along with an Advisory Commission on Critical Trends Analysis. The office would identify and analyze critical trends and alternative futures based largely on information obtained from Federal departments and agencies, as well as on outside sources of information. The office would advise the President and issue various reports on the key trends and their relationship to present and future problem areas, opportunities, and policy options. The act also would require the Joint Economic Committee of Congress to prepare a legislative branch report on critical trends and alternatives futures.[75]

S. 1031 was introduced by Senator Albert Gore at a joint hearing of the Senate Governmental Subcommittee on Governmental Efficiency, chaired by Senator Charles McC. Mathias, and the Senate Committee on Environment and Public Works, chaired by Senator Robert Stafford. The Aprii 30th hearing highlighted some of the major arguments for and against government foresight and a governmentwide foresight office. Basically, none of the witnesses argued that there should be no government foresight. All agreed that government policymaking should take into account the best available information and analyses concerning the future. All agreed that computer modeling has a legitimate role in foresight and policymaking, although views differed on the importance of this role.

DOE Deputy Secretary Danny Boggs highlighted the limitations of models due to inferior or incomplete input data, mathematical and conceptual errors in building the model, and inadequate theoretical understanding of the processes being modeled. He believes that advances in computing power have outstripped advances in the theoretical underpinning of computer modeling. Mr. Boggs also expressed concern about the apparent bias in computer models, and especially global computer models, toward a negative future, and cited several previous energy supply, demand, and price forecasts (both governmental and private sector) that have proven to be far too pessimistic. Mr. Boggs cited the efforts of the EIA to improve the quality of computer-based models and forecasts.[76]

---

[74] Ibid.; U.S. Congress, House of Representatives, Committee on Science and Technology, Subcommittee on the Environment and the Atmosphere, *Long Range Planning*, a report prepared by CRS, 94th Cong., 2d sess., May 1976; U.S.Congress, House of Representatives, Committee on Energy and Commerce, *The Strategic Future: Anticipating Tomorrow's Crises*, a report prepared by CRS, 97th Cong., 1st sess., August 1981; U.S. Congress, House Committee on Energy and Commerce, *Strategic Issues: Historical Experience, Institutional Structures and Conceptual Framework*, a report prepared by CRS, 97th Cong., 2d sess., July 1982; U.S. Congress, House, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations and Subcommittee on Oversight and Investigations and Subcommittee on Energy Conservation and Power, *Public Issue Early Warning Systems: Legislative and Institutional Alternatives*, hearings and workshop, 97th Cong., 2d sess., October 1982; U.S. Congress, House, Committee on Science and Technology, *Subjects and Policy Areas for the Consideration of the House Committee on Science and Technology*, a report prepared by CRS, 98th Cong., 1st sess., April 1983.

S. 1031, the Critical Trends Assessment Act, Apr. 30, 1985, 99th Cong. 1st sess. For discussion of prior legislative initiatives, see, for example, Lindsey Grant, *Thinking Ahead*, op. cit.; and Joseph F. Coates, "Foresight," op. cit.

Senator Gore emphasized that a Critical Trends Office would not be a central planning agency trying to impose a uniform view of the world, but would help the government make more effective use of the already substantial level of data collection and modeling activity. Mr. Lindsey Grant, a former Deputy Assistant Secretary of State, testified that such an office could help improve understanding of what databases and models already exist and how these resources could be used for more informed government policymaking. Senator Mathias outlined what he views as the high payoff of improved global foresight in areas such as long-term export and import needs of U.S. trading partners; long-term supply and demand for energy and food; and preparing for and responding to natural disasters such as crop-freezes, earthquakes, floods, and droughts.[77]

OTA did not analyze the various institutional options. However, three things seem clear. First, many of the applications of information technology considered throughout this chapter (as well as, to some extent, throughout ch. 7 on electronic databases and dissemination of government information) are likely to make the job of any potential governmentwide foresight office more feasible than in the past. Second, many of the options for improved decision support (e.g., guidelines on model evaluation, clearinghouse or index to major models and databases, testing and development of decision conference techniques) considered earlier are also likely to facilitate improved foresight—both agency-specific and governmentwide. Three, in order to realize the potential for improved foresight, some strengthened central coordinating mechanism appears to be necessary in order to ensure high-level support, adequate agency cooperation, and effective implementation of whatever specific measures are agreed to by Congress and the President.

---

[76] See testimony of Danny J. Boggs, Deputy Secretary, U.S. Department of Energy, before the Apr. 30, 1985, joint hearing on "Global Forecasting Capability of the Federal Government," conducted by the Subcommittee on Government Efficiency of the Committee on Governmental Affairs, and the Committee on Environment and Public Works, U.S. Senate.

[77] See statements of Senator Albert Gore, Senator Charles McC. Mathias, and Mr. Lindsey Grant before the joint hearing, ibid.

Chapter 7

Electronic Databases and Dissemination of Government Information

Contents

Page

Summary 139

Introduction 140

Key Trends 140
- Continuing Importance of Government Information 140
- Reduction of Paperwork and Publications 141
- Growing Role of the Private Sector 142
- Increasing Use of Electronic Dissemination 143
- Agency Planning for Government Information Revolution 145

Key Issues 147
- Further Study of Cost-Effectiveness of Electronic Information Options 147
- Equity of Access to Electronic Government Information 147
- Private Sector Role in Federal Electronic Information Activities 148
- Institutional Responsibility for Government Information Policy and Operations 150
- Public Information Index or Clearinghouse 152
- Mechanisms for Exchange of Learning and Innovation 152
- Freedom of Information Act Implementation 153
- Electronic Recordkeeping and Archiving 155
- Scientific and Technical Information 156
- Other Issues 158

Table

Table No. *Page*

7-1. Illustrative Agencies With Some Electronic Dissemination of Public Information 144

Chapter 7

Electronic Databases and Dissemination of Government Information

SUMMARY

The importance of the public information functions of the Federal Government has been recognized since the founding of the Republic. Congress has taken a long series of actions to institutionalize these functions, by establishing, for example, the national libraries (of Congress, Medicine, and Agriculture), Government Printing Office, Federal Depository Library Program, and National Technical Information Service, and enacting laws such as the Public Printing Act, Freedom of Information Act, Federal Program Information Act, and Government in the Sunshine Act.

Public information, that portion of government information that is not personal, proprietary, or classified (or otherwise subject to Freedom of Information Act (FOIA) exemptions), is vital to the missions of virtually every department and agency of government, and runs the gamut from reports, periodicals, directories, and handbooks; to rules, regulations, and circulars; to scientific and technical information, statistical data, satellite imagery, and computer models; to maps, charts, and photographs.

However, new public information issues are being raised (and old ones exacerbated) by the confluence of several key trends: the continuing importance of public information; the reduction of paperwork and publications (in part due to requirements of the Paperwork Reduction Act (PRA) and Deficit Reduction Act); the growing role of the private sector (which depends heavily on the use of modern information technology); and the increasing Federal agency use of electronic collection, maintenance, and dissemination of public information.

Use of information technology—such as electronic document filing, computer-aided surveys, computerized databases, optical disks, electronic mail, electronic remote printing, and electronic bulletin boards—could revolutionize the public information functions of government. There are already numerous Federal agency pilot projects, and some of the more visible ones have generated intense controversy. Once again, the issues are complicated because of inherent tensions involving public access and the public's right to know, the role of Federal agencies in actively disseminating public information, management efficiency and cost reduction, private sector cooperation and competition, and, particularly for scientific and technical information, national security and foreign trade concerns.

OTA concluded that further research in this area is warranted, but that, ultimately, Congress is likely to be called on to update existing public information laws and address a variety of issues, such as:

- the cost-effectiveness of electronic information options;
- the equity of access to electronic government information;
- the private sector role in Federal electronic information activities;
- the institutional responsibility for policy and operations concerning government information collection and dissemination;
- the need for a public information index or clearinghouse;
- mechanisms for exchange of learning from innovative electronic information activities;
- use of information technology in Freedom of Information Act implementation;

- electronic recordkeeping and archiving;
- scientific and technical information exchange; and
- other issues—transborder information flow, depository library system, Federal statistical system, and copyright protection.

OTA also reviewed innovative activities in selected States (Michigan, Virginia, Oregon, North Carolina, California, and Florida) and localities (Lane County, Oregon; Columbus, Ohio; and Beverly Hills, Irvine, Palos Verdes, and Buena Park, California). The results, combined with those from OTA's Federal Agency Data Request, indicate that information technology can facilitate public access to government information. Two applications appear to have noteworthy potential:

1. electronic access to information about the process and results of government activities, especially decisionmaking activities; and
2. access (electronic where feasible) to the databases and computer models used by government agencies to develop and evaluate options and formulate positions on various issues. (See ch. 6 for related discussion.)

This potential depends in good part on an interested and educated citizenry, as well as on the absence of technical and cost barriers. Nonetheless, information technology appears to offer significant potential to implement public access to, as well as dissemination of, government information.

INTRODUCTION

Information technology holds out the promise of faster, cheaper, and more efficient collection (e.g., through computer-aided surveys or document filings), storage (e.g., in computerized databases, optical disks), and dissemination of government information (e.g., via electronic mail, interactive data networks, electronic bulletin boards, remote printing-on-demand, and computer tape exchange). OTA's preliminary research in this area suggests that the Federal Government is at or near the threshold of a major transition toward greater use of information technology for managing government information.

At the same time, because government information is vital to so many users—in and outside of government—and central to numerous public laws and agency missions, this transition is being closely watched and is raising a wide range of issues. Indeed, several pilot projects have become highly controversial. This is in large part because the policy framework for agency applications (e.g., electronic filing, database creation, and remote printing) is *not* clear.

OTA concluded that the technological possibilities, institutional alternatives, and policy options deserve further research attention, but that, ultimately, Congress is likely to be called on to update existing public laws—or enact new ones—for this emerging Federal electronic information environment.

The results of OTA's preliminary research on this topic are presented below, including a discussion of key trends and issues.

KEY TRENDS

Continuing Importance of Government Information

The transition of the Federal Government from paper-based to greater electronic collection, maintenance, and dissemination of information is controversial because of the importance placed on government information itself.

For purposes of this analysis, OTA defined "government information" as information collected and/or developed at Federal Government expense (i.e., with public funds) to carry out government functions and agency missions (whether or not the information itself is explicitly authorized or required by statute). Government information includes everything that is legally available to the public, as well as those specific types of information restricted from public access under the Freedom of Information Act exemptions (e.g., law enforcement, investigative, confidential, proprietary, and classified information). In this preliminary research, OTA focused primarily on government information that is publicly available, i.e., "public" information. Such information runs the gamut from statistical data, computer models, reports, periodicals, directories, and handbooks; to rules, regulations, and circulars; to maps, charts, and photographs.[1]

The importance of the public information functions of the Federal Government has been recognized since the founding of the Republic. Congress has taken a long series of actions to institutionalize these functions, as illustrated by the establishment of the Library of Congress in 1800, Library of the Surgeon General's Office in 1836 (later to become the National Library of Medicine), Government Printing Office (GPO) in 1860, National Agricultural Library in 1862, Federal Depository Library Program in 1913, and National Technical Information Service in 1970.[2]

In addition, Congress has articulated the importance of access to and dissemination of public information in enacting, for example, the Freedom of Information Act in 1966, Public Law 91-345 establishing the National Commission on Libraries and Information Science in 1970, the Federal Program Information Act (concerning information about Federal assistance programs), and the Government in the Sunshine Act in 1976.[3]

Congress has enacted numerous public laws assigning public information functions to specific Federal agencies. According to the Congressional Research Service, Congress enacted a total of 92 laws during the last four Congresses (95th through 98th) on government information systems, clearinghouses, and dissemination. In the 98th Congress alone these laws spanned the information spectrum from alcohol and drug abuse, education of the handicapped, smoking health hazards, and adult and vocational education to arctic research, water resources, and hazardous waste control.[4] As further illustration, 28 bills on public information topics had been introduced in just the first 6 months of the 99th Congress, that, if enacted, would establish the following kinds of government information activities (some bills proposed more than one kind of activity):[5]

- provide information on request (9 bills),
- establish information clearinghouse (8),
- collect information (8),
- disseminate information (7),
- establish national database or directory (5), and
- establish uniform information reporting procedures (5).

Reduction of Paperwork and Publications

Congress has also expressed the desire to reduce the paperwork burden of the Federal Government and redundancy or inefficiency in government data collection efforts, as reflected in enactment of PRA in 1980. In addition, the Office of Management and Budget (OMB) has led a strong effort to reduce the cost of government public information activities, in part on its own initiative[6] and in part in response to the Paperwork Reduction Act of 1980 (with respect to information collection activities) and the Deficit Reduction Act of 1984 (with respect to publishing, public affairs, and audiovisual activities).

---

[1] For a complete discussion of definitions and types of government information, see Charles R. McClure and Peter Hernon, *Federal Government Provision of Public Information: Issues Related to Public Access, Technology, and Laws/Regulations*, OTA contractor report, Dec. 28, 1984.

[2] See Ibid.; and Marilyn Gell Mason, *The Federal Role in Library and Information Services* (White Plains, NY: Knowledge Industry Publications, 1983).

[3] Ibid.

[4] Sandra N. Milevski and Robert L. Chartrand, "Information Policy: Legislation of the 95-98th Congresses, With Selected Bills of the 99th Congress," Congressional Research Service, Library of Congress, June 1985.

[5] Sandra N. Milevski, CRS, June 1985.

[6] See, for example, Office of Management and Budget, "Elimination of Wasteful Spending on Government Periodicals, Pamphlets, and Audiovisual Products," Bulletin No. 81-16, Apr. 21, 1981; and Office of Management and Budget, "Elimination and Consolidation of Government Periodicals and Recurring Pamphlets," Bulletin No. 81-16, Supplement No. 1, Oct. 9, 1981.

OMB claims that 3,848 of the approximately 10,000 publications in the Federal inventory have been eliminated or consolidated and another 3,100 have been cut back.[7]

With respect to paperwork reduction, OMB has given priority to reducing the paperwork burden (specific annual reduction goals were included in the act) defined in terms of the "information collection budget," that is, the number of hours estimated to fill out government forms. OMB claims a net reduction of 36 percent in the paperwork burden between 1980 and 1984.[8]

In combination with the Administration's program to reduce fraud, waste, and abuse, OMB worked to eliminate or consolidate 3,848 government publications (as noted above) and close or downgrade 111 government printing plants. In response to the Deficit Reduction Act of 1984, OMB is proposing further reductions in publishing and audiovisual activities and in public affairs activities. However, the amount of the reductions is less than that suggested by the act, because, according to OMB, any further reductions would compromise essential agency missions.[9]

To provide further confirmation of reported reductions, OTA asked agencies to provide (to the extent available) budget, staffing, and activity data for printing and publishing in fiscal years 1980 and 1984 (actual by year), 1985 (projected), and 1986 (anticipated). The completeness of the responses varied widely, but many agencies did indicate a reduction in staff, and frequently in budget as well, for printing and publishing, along with a reduction in the number of titles and copies prepared.[10]

These developments have, to some extent, given more impetus to examining electronic alternatives to paper-based public information systems, on the premise that electronic alternatives will be less costly and more effective.

Growing Role of the Private Sector

The role of information technology (e.g., computers, telecommunications, and electronic printing) in the larger sense has been as a catalyst of change. The technology has vastly expanded the options for the collection, maintenance, and dissemination of all kinds of information, including public information, and has helped spawn a new industry—the "information industry." This industry depends heavily on the use of modern information technology and is aggressively seeking opportunities to serve all markets—including the public information market. Thus, there are now numerous private companies that seek to provide public information products or services, either under contract to the government, in competition with the government, and/or as a complement to the government by adding value to or repackaging government information.

The Information Industry Association (IIA), a trade association representing information publishers and providers of all varieties, claims that U.S. information companies had revenues in 1983 of $13 billion, growing at 20 percent per year. The IIA has over 450 members, including firms like Chase Econometrics, Dun & Bradstreet, University Microfilms, McGraw-Hill, Dow Jones, and Congressional Information Service.[11]

---

[7] Office of Management and Budget, *Management of the United States Government: Fiscal Year 1986*, January 1985, pp. 17-18.

[8] Office of Management and Budget, *Managing Federal Information Resources*, third annual report under the Paperwork Reduction Act of 1980, June 1984, pp. 8-9; and Office of Management and Budget, *Information Collection Budget of the United States Government*, fiscal year 1985, Apr. 12, 1985.

[9] OMB, *Management of the U.S. Government*, op. cit., pp. 88-91. Some groups, such as Ralph Nader's Public Citizen, believe that public information cutbacks have already significantly impaired agency functions. See Public Citizen, *Starving for Nutrition Information From Reagan's USDA*, August 1984; Public Citizen, *Gasping for Information at Reagan's EPA*, October 1984; and Public Citizen, *Lights Out at DOE: How Reagan Has Put America in the Dark About Energy*, November 1984.

[10] Based on the response of 125 agency components to OTA's Federal Agency Data Request.

[11] Testimony of Peter Marx on behalf of the Information Industry Association before U.S. House of Representatives, Com-

Thus, the information industry seeks to use information technology to help meet public information needs generally on a commercial, for-profit basis. At the same time, public information advocates, such as librarians and university researchers, are concerned that private industry involvement in electronic collection, maintenance, and dissemination of government information may serve to reduce the availability of that information.[12]

Issues raised by the private sector role in the provision of government information have stimulated a large number of conferences, reports, and hearings. For example, in 1982, the National Commission on Libraries and Information Science published a report on *Public Sector/Private Sector Interaction in Providing Information Services*.[13] Later in 1982, OTA published a technical memorandum on *MEDLARS and Health Information Policy*, which gave major attention to public/private issues.[14] In 1983, the Library of Congress published a report on *Public/Private Interactions: The Implications for Networking*.[15] As a final example, in 1984, OTA issued a technical memorandum on *Remote Sensing and the Private Sector*.[16] There have also been several congressional hearings on the topics of government provision of public information in competition with the private sector;[17] the Securities and Exchange Commission's Electronic Data Gathering, Analysis, and Retrieval system (EDGAR);[18] electronic collection and dissemination of government information;[19] and OMB's draft and final circulars on "Management of Federal Information Resources," in which the private sector is assigned a central role.[20]

Increasing Use of Electronic Dissemination

OTA found that a significant percentage of Federal agencies (roughly 40 percent of agencies responding to OTA's Federal Agency Data Request) make available or disseminate some public information in an electronic format. The nature and extent of such electronic dissemination varies widely. Of those responding, 47 of 118 agency components reported some electronic activity, including all of the largest public information providers and all of the major Federal statistical agencies, as illustrated in table 7-1.

The most common electronic dissemination activities involve the use of electronic mail (or the equivalent) for the distribution of press releases, bulletins, notices, and short reports, and the use of computer tapes for distribution of statistical databases and reports. Some examples follow:

- *Economic Research Service (Department of Agriculture)*—Outlook and Situation

---

mittee on Energy and Commerce, Subcommittee on Oversight and Investigations, Mar. 14, 1985, p. 1. Also see A.C. Nielson, *The Business of Information*, report prepared for the Information Industry Association, 1983.

[12] For a summary of concerns expressed by librarians, researchers, and others in response to OMB's draft circular on "Management of Federal Information Resources," see *Information Hotline*, special feature, vol. 17, No. 9, October 1985.

[13] U.S. National Commission on Libraries and Information Science, *Public Sector/Private Sector Interaction in Providing Information Services*, February 1982.

[14] U.S. Congress, Office of Technology Assessment, *MEDLARS and Health Information Policy—A Technical Memorandum*, OTA-TM-H-11 (Washington, DC: U.S. Government Printing Office, September 1982).

[15] U.S. Library of Congress, Network Development Office, *Public/Private Sector Interactions: The Implications for Networking*, prepared by the Network Advisory Committee, 1983.

[16] U.S. Congress, Office of Technology Assessment, *Remote Sensing and the Private Sector: Issues for Discussion—A Technical Memorandum*, OTA-TM-ISC-20 (Washington, DC: U.S. Government Printing Office, March 1984).

[17] U.S. Congress, House of Representatives, Committee on Government Operations, Subcommittee on Government Information and Individual Rights, *Government Provision of Information Services in Competition With the Private Sector*, hearing, 97th Cong., 2d sess., Feb. 25, 1982; see also Representative Glenn English, "Electronic Filing of Documents With the Government: New Technology Presents New Problems," *Congressional Record—House*, Mar. 14, 1984, H 1614-1615.

[18] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, hearing, Mar. 14, 1985.

[19] See, for example, U.S. Congress, House Committee on Government Operations, Subcommittee on Government Information, hearing, Oct. 18, 1985.

[20] See, for example, U.S. Congress, House Committee on Government Operations, Subcommittee on Employment and Housing, hearing, July 17, 1985. Also see Office of Management and Budget, "Management of Federal Information Resources" *Federal Register*, vol. 50, No. 51, Mar. 15, 1985. The final version was issued on Dec. 12, 1985.

Table 7-1.—Illustrative Agencies With Some Electronic Dissemination of Public Information

- *Department of Agriculture*
  - Economic Research Service
  - Statistical Reporting Service
  - Food and Nutrition Service
  - Human Nutrition Information Service
  - Rural Electrification Administration
- *Department of Commerce*
  - Census Bureau
  - Bureau of Economic Analysis
  - International Trade Administration
  - National Bureau of Standards
  - National Technical Information Service
  - Patent and Trademark Office
- *Department of Energy*
  - Energy Information Administration
  - Federal Energy Regulatory Commission
- *Department of Health and Human Services*
  - National Center for Health Statistics
  - Centers for Disease Control
  - Food and Drug Administration
  - Social Security Administration
- *Department of the Interior*
  - Fish and Wildlife Service
  - U.S. Geological Survey
  - Bureau of Mines
- *Department of Justice*
  - Bureau of Justice Statistics
  - National Institute of Justice
- *Department of Labor*
  - Bureau of Labor Statistics
- *Department of Transportation*
  - National Highway Traffic Safety Administration
  - Urban Mass Transportation Administration
- Consumer Product Safety Commission
- Federal Communications Commission
- Federal Election Commission
- Federal Emergency Management Agency
- Federal Reserve System
- National Aeronautics and Space Administration
- Small Business Administration

SOURCE: Office of Technology Assessment

reports are electronically disseminated through AGNET, a computer system operated by the University of Nebraska. The reports are 32 to 40 pages in length (text and tables), number roughly 100 per year, and are also available for purchase in hardcopy form through GPO. The electronic reports are derived directly from the ERS word-processing system, transmitted to AGNET, and available via dial-up telecommunications. AGNET controls the fees and access. Users range from individual farm operators to the Government of New Zealand to value-added information providers (e.g., agricultural newsletters).

- *Bureau of the Census (Department of Commerce)*—Selected Census data are available on-line via a commercial vendor—Dialog Information Services and the Glimpse Corp. Called CENDATA, the on-line dial-up service also includes Bureau news releases, user news bulletins, and product information. Census anticipates that CENDATA offerings will gradually increase over time. Census also sells data sets in computer tape and diskette format, and distributes the data tapes at no charge to the 50 State census data centers.
- *National Bureau of Standards (Department of Commerce)*—Various computer tapes generated by NBS scientists and engineers are made available through the National Technical Information Service (NTIS). Also, the NBS National Standard Reference Data System provides databases (of physical and chemical properties of substances) on magnetic tapes and through on-line computer networks, as well as in printed form.
- *Various Health and Human Services Agencies*—The National Center for Health Statistics makes over 400 data files available on computer tape, generally via NTIS. The Food and Drug Administration uses ITT Dialcom for an "electronic bulletin board" on a trial basis; electronic notices are also available in paper form. The Social Security Administration places selected SSA data in a Compuserve information service that is available on a dial-up basis.
- *National Highway Transportation Safety Administration (Department of Transportation)*—NHTSA maintains a Vehicle Biomechanics Testing Data Base that started in 1978 and currently contains data on 800 vehicle crash tests and 900 occupant crash tests. The database is available directly from NHTSA via computer tape and dial-up access, and is free. NHTSA also has a toll-free Auto Safety Hotline for consumer safety information, and

manages a technical reference service for highway safety information.

- *National Aeronautics and Space Administration*—NASA has offered NASA NEWS since fall 1984. NASA NEWS is an electronic database containing press releases, shuttle status reports, flight schedules, etc.; it is available on a dial-up basis from NASA headquarters and field offices via the NASA contractor, Dialcom. Users include government agencies, contractors, news media, and libraries. NASA also maintains an aerospace database that includes about 1.5 million references and abstracts of reports and journal articles. The database is available in computer tape format via commercial vendors working under an arrangement with the American Institute of Aeronautics and Astronautics (the NASA contractor).

Agency Planning for Government Information Revolution

Despite the fairly widespread agency use of electronic dissemination of government information, such use is still largely in the formative stages. Electronic information accounts for only a small percentage of the total government information flow. However, the results of OTA's Federal Agency Data Request and examination of selected agency activities and plans strongly suggest that major changes are likely. Several agencies are experimenting with various new technologies and planning for expanded use of several that bear directly on government information functions.

The heaviest area of current activity appears to be with respect to computerized databases. There are estimated to be several thousand in the Federal Government already, and several agencies are studying new or expanded use of computerized databases.

As an illustration of a recently completed (March 1985) study, the Federal Election Commission (FEC) evaluated a pilot project on direct electronic access to Federal campaign finance data. The pilot project permits eight State campaign finance offices in seven States to access FEC data directly. The study concluded that this concept could be usefully extended so that FEC data would be electronically available at terminals in all States and major cities. This is viewed by the FEC as enhancing the mission objective of making Federal campaign finance data widely available to government officials, the media, candidates, political action committees, party committees, academics, and researchers.[21] Continuation of the electronic access project is uncertain in light of possible agency budget reductions.

A March 1984 NBS workshop on the effect of computers on the generation and use of technical data concluded that technical databases are essential to U.S. industry and that electronic dissemination has significant advantages. These include the ability to locate desired data more reliably and quickly, update the data in a more timely fashion, and transfer the data more accurately and less expensively.[22]

As a third example, in 1984, the Federal Communications Commission (FCC) concluded an inquiry into the possibility of allowing the public direct electronic access to FCC computerized databases. Various respondents expressed the desire to have faster and more accurate access to FCC data of interest. After deliberating on cost, technical, security, and other considerations, FCC decided to select a contractor to make certain that their files were available to the public on a commercial basis at a reasonable cost, with NTIS acting as account manager for a third-party contract between the FCC and a vendor.[23]

As a final example, the National Center for Health Statistics (NCHS) has a well-developed publications survey form. The form goes out over the signature of the NCHS Director and asks respondents, among other things, if they are not interested, somewhat interested, or very interested in purchasing NCHS information by:[24]

---

[21] U.S. Federal Election Commission, *State Computer Access to FEC Federal Campaign Finance Data: Report of a Pilot Project*, March 1985.

[22] U.S. Department of Commerce, National Bureau of Standards, *The Effect of Computers on the Generation and Use of Technical Data*, report of a workshop, June 1984.

[23] U.S. Federal Communications Commission, General Docket No. 83-483, Report and Order, In the Matter of Allowing the Public Direct Remote Access to Commission Computer Data Bases, Aug. 13, 1984.

- *electronic release*—direct access through computer terminals to the latest NCHS data in summary or detailed form;
- *direct computer access* to NCHS reports prior to publication;
- *automated bibliographic system*—direct access through computer terminals to an index of NCHS published and unpublished data to determine the availability of specific types of data;
- *data networks*—access to printed and computer products, as well as assistance in locating and using data at a regional or State center on a cost basis; and
- *phone-in data line*—a users call-in service for obtaining the latest summary data on selected topics, such as monthly vital statistics data.

Several of these applications come very close to, if not actually embracing, printing-on-demand or remote electronic printing—whereby, for example, government documents would be stored in electronic form and transmitted electronically to the location of the user where a hardcopy would be printed out. In response to the OTA Federal Agency Data Request, 21 out of 114 agencies reported use of printing-on-demand or remote electronic printing. It appears that such use is primarily for internal purposes at the present time, but the opportunities for use in dissemination of government information are significant. A 1982 study prepared for the Energy Information Administration concluded that they were not taking advantage of electronic publishing options that could reduce costs and increase quality and timeliness.[25] Private sector development and use of electronic printing and publishing technologies are growing rapidly.[26]

In addition, agencies already report significant use of electronic mail and audioconferencing, and emerging use of computer-conferencing, videoconferencing, and optical disks. All of these technologies have direct application to dissemination of government information. The number of agencies using optical disks is projected to quintuple, the number using videoconferencing is projected to triple, and the number using computer-conferencing is projected to double, based on current plans.

	Current use		*Planned use*	
Technology	*Number**	*Percent*	*Number*	*Percent*
Electronic mail	97	72%	115	86%
Audioconferencing	84	63	86	64
Computer-conferencing	16	12	29	22
Videoconferencing	10	8	30	22
Optical disks	6	4	39	29

*Based on 134 agencies responding to this part of OTA's Federal Agency Data Request.

In sum, the actions and plans of individual Federal agencies clearly indicate that electronic information technology is destined to become an increasingly significant part of government information functions. A good illustration is the year 2000 planning scenario of the Defense Technical Information Center (DTIC), summarized below:[27]

> DTIC will be a highly automated operation where the vast majority of data transfers are electronic. It will be situated in an environment where all users have access to computer work stations; where computer storage has the density, access speeds, and reliability to permit full-text storage of all items; . . . where mailing of paper products has been replaced by electronic transmissions; [and] where the power/speed of computers and the sophistication of software eliminate the need for both manual indexing and development of intricate search strategies.

---

[24] U.S. Department of Health and Human Services, Public Health Service, National Center for Health Statistics, *NCHS Publications Survey*, no date.

[25] Henry B. Freedman, *A Technology Assessment of Electronic Publishing Options for the Energy Information Administration National Energy Information Center*, March 1982.

[26] See, for example, Andrew Parker, "A Colourful Revolution in Printing," *New Scientist*, Sept. 26, 1985, pp. 52-55; Erik Sandberg-Diment, "Desktop Publishing Comes of Age," *New York Times*, Nov. 26, 1985, p. C4; Johanna Ambrosio, "Publishing In-House Can Sharpen DP Image," *Computerworld*, Dec. 2, 1985; and Patricia McShane, "Printing With Light Speed," *Computer Decisions*, Dec. 17, 1985, pp. 78-81.

[27] U.S. Department of Defense, Defense Logistics Agency, Defense Technical Information Center, *DTIC 2000: A Corporate Plan for the Future*, DTIC/TR-84/3, July 1984.

KEY ISSUES

OTA identified several issues that warrant further study and may, ultimately, require congressional action. The purpose here is to identify issue areas and some possible options—not to analyze the issues in depth or develop and evaluate options in any detail.[28]

Further Study of Cost-Effectiveness of Electronic Information Options

Many agencies are moving ahead on the assumption and belief that electronic collection, maintenance, and dissemination of government information is cost-effective. The results of those agency studies reviewed by OTA suggest that this may be the case. However, most agencies engaged in electronic dissemination have not conducted such a study; nor has there been a governmentwide study on this topic.

Based on the results of the OTA Federal Agency Data Request, only 10 agencies (9 percent of all 125 agencies responding; 21 percent of agencies using electronic dissemination) report any kind of study on the impacts of electronic dissemination.

If indeed the information currently available is not adequate as a basis for public policymaking, one or more of the following options could be pursued:

1. further studies by specific agencies (e.g., in the process of authorization and appropriation actions);
2. preparation of a governmentwide report by one of the central agencies (e.g., Office of Information and Regulatory Affairs/OMB; Office of Information Resources Management/General Services Administration (GSA); Institute for Computer Science and Technology/NBS); and/or
3. studies by one or more of the congressional support agencies (i.e., Congressional Budget Office, Congressional Research Service, General Accounting Office (GAO), OTA).

Equity of Access to Electronic Government Information

One of the most basic issues involves the extent to which electronic options affect the relative availability of government information to various publics. As noted earlier, the importance of government information is reflected in numerous public laws, but also in the strongly held views of librarians, educators, researchers, public interest groups, the press, and others who believe that government information is an important public good and central to the fabric of American society.[29]

The core issue is whether the shift from a substantially paper-based to a largely electronic-based government information system will, absent policy intervention, create new inequities and barriers to access. One concern is that electronic dissemination will advantage primarily those with the funds and/or technical sophistication needed to use computerized databases. This concern is amplified to the extent that electronic dissemination is viewed as a luxury or special service and offered on a cost recovery and/or market pricing basis. An alternative approach would be to establish the electronic format as the primary format, to be widely accessible by citizens and interested publics, with paper copies viewed as a luxury or special service.

---

[28] For further discussion, see McClure and Hernon, *Public Information*, op. cit. Also, OTA has already been asked to examine many of these issues in detail, as outlined in a letter from Senator Charles McC. Mathias, Chairman, and Representative Frank Annunzio, Vice Chairman of the Joint Committee on Printing, U.S. Congress, to OTA Director John H. Gibbons, dated May 17, 1985. Related letters of request were sent to the General Accounting Office and Government Printing Office with respect to work complementary to that requested of OTA.

[29] See, for example, Lewis M. Helm, Ray Eldon Hiebert, Michael R. Naver, and Kenneth Robin, *Informing the People* (New York: Longman, 1981); Donna A. Demac, *Keeping America Uninformed: Government Secrecy in the 1980's* (New York: The Pilgrim Press, 1984); Carol A. Tauer, "Social Justice and Access to Information," *Minnesota Libraries*, summer 1982, pp. 39-42; Marc A. Levin, "Access and Dissemination Issues Concerning Federal Government Information," *Special Libraries*, April 1983, pp. 127-137; Mimi Abramovitz, "Secrecy in the Welfare State," *Social Policy*, spring 1985, pp. 52-55; numerous statements submitted in response to OMB's draft circular on "Management of Federal Information Resources" as abstracted in *Information Hotline*, October 1985; and Eugene Garfield, "Society's Unmet Information Needs," *ASIS Bulletin*, October/November 1985, pp. 6-7.

In reality, the situation is far more complex, since there is a range of users with different needs, motivations, and abilities to pay. For example, the additional cost of obtaining financial information from the Securities and Exchange Commission (SEC) in electronic form may be insignificant to a trade association or private firm, but substantial to a graduate student or researcher. And the value of information to the government and the user also varies widely. Thus, public policy may determine that health and safety information should be disseminated without cost to the user and as expeditiously as possible, whereas trade or industrial market information should be priced on a full cost-recovery basis.

In sum, the equity issue is complex, and involves a wide range of government information categories, public policy objectives, user groups, and dissemination technologies. At present, Federal agencies formulate their public information strategies within an equally complex set of public laws and OMB rules and regulations. The shift to electronic collection, storage, and dissemination strategies appears to be aggravating these already difficult policy choices, to the extent that Congress may need to provide revised or new guidance.

Private Sector Role in Federal Electronic Information Activities

Another basic issue involves the appropriate role (or, more realistically, roles) of private firms in the collection, maintenance, and dissemination of government information. The information industry is predicated on the use of information technology, and as the government shifts to greater emphasis on using the technology, opportunities for conflict, competition, and cooperation will inevitably increase.

An example of cooperation is the Department of Agriculture (USDA) electronic database for time-sensitive data such as market, crop, and livestock reports, economic outlook reports, and the like. USDA contracted for a private vendor on a competitive basis, and ultimately selected Martin Marietta Data Systems. Martin Marietta agreed to utilize standard rates, accept whatever data USDA placed on the system, release the data for equal access to all users, according to the USDA schedule, and delete the data when requested by USDA. Martin Marietta further agreed to an anti-competitive provision prohibiting its resale of the data at retail, thus removing a potentially unfair competitive advantage. The system provides data and reports instantaneously in electronic format. This is an example where the government agency (USDA) has retained complete control over the data. But even here, an equity issue still exists because users who want instant electronic access must pay an extra charge, however nominal ($150 per month minimum fee), and must have an electronic terminal, thus potentially disadvantaging users who lack the money, equipment, or both.[30]

An example of competition is the Department of Labor (DOL) proposal to make key statistical data on the labor force, price indices, unemployment, and the like available to the public in on-line electronic format via NTIS. The data were to have been provided in chart and tabular as well as raw form. A private firm, Data Resources, Inc., saw this proposal as direct competition and opposed implementation. In part as a result, DOL withdrew the proposal.[31] But this situation raises the issue of whether and when government provision of public information should be limited to those areas where there is no current or potential private vendor.

Finally, two examples of conflict are the electronic filing project of SEC and the electronic trademark database project of the Patent and

---

[30] Roxanne Williams, "Getting the Word Out: The Agriculture Department's New System for Electronic Dissemination of Time Sensitive 'Perishable' Data," *Government Data Systems*, June/July 1985, pp. 28-29; "USDA's Computerized Information Service," *Information Hotline*, September 1985, pp. 3-4.

[31] Reinhardt Krause, "Policy Shift: Using the Private Sector to Market Federal Databases," *Government Data Systems*, June/July 1985, pp. 25-26.

Trademark Office (PTO). In both cases, automation is generally regarded as potentially cost-effective. But SEC sought to finance the computerized system for corporate filings through an exchange agreement with a private vendor, whereby the vendor would recover the costs of system development and operation through user fees for basic services and sales of value-added services. The vendor would have exclusive rights to the sale of on-line bulk data. Likewise, PTO sought to finance the preparation of a computerized database for its trademark registration information by exchange agreements with private vendors, whereby the vendors would receive free copies of present and future trademark information and be granted restrictions on public access to advanced search functions. This apparently was intended to protect the vendors' value-added markets. PTO subsequently relaxed the public access restrictions, but imposed a royalty fee that was to be passed on to the vendors.[32]

The SEC and PTO electronic information projects have raised numerous questions, such as the impact on public access and industry competition; the use or misuse of exchange agreements; whether Federal procurement laws and regulations have been properly followed; the adequacy of cost-benefit and feasibility studies; potential conflict of interest with vendors; and whether and under what conditions vital government information should be under the control of, and accessible only through, private firms.[33]

In a broader context, these issues are particularly significant given that the OMB draft circular on "Management of Federal Information Resources" emphasizes reliance on the private sector and user charges. For example, the circular, while recognizing that government information dissemination can be necessary and even essential to agency missions, permits such dissemination by the government itself only if the information product or service is not already provided by other government or private sector organizations or could not reasonably be provided by such organizations in the absence of agency dissemination.[34] And, while the draft circular notes that dissemination should be conducted "in a manner that reasonably ensures the information will reach . . . the public . . . ," the circular requires that "maximum feasible reliance" be placed on the private sector for dissemination and that costs of dissemination be recovered through user charges, where appropriate.[35]

The final version of the OMB circular issued in December 1985 gives more explicit recognition to the importance of government information. For example, the circular states that "government information is a valuable national resource," and "[t]he free flow of information from the government to its citizens and vice versa is essential in a democratic society."[36] However, the circular still places heavy emphasis on the private sector. Thus, Federal agency dissemination must be either "[s]pecifically required by law" or "[n]ecessary for the proper performance of agency functions," provided that the information products and services disseminated "do not duplicate similar products or services that are or would otherwise be provided by other government or private sector organizations."[37] The circular continues to require that "maximum feasible reliance" be placed on the private sector for dissemination, and that costs be recovered through user charges, where appropriate.[38] The final version of the circular cites OMB Circulars A-76 and A-25 as authorities for maximum feasible reliance on the private sector and for user charges. The draft version implied that these provisions were based on the Paperwork Reduction Act or other general statutory authority.

---

[32] On the SEC project, see statements of James Watts of GAO and Peter Marx of the Information Industry Association before the Mar. 14, 1985, hearing of the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce; on the PTO project, see U.S. Comptroller General, *Patent and Trademark Office Needs to Better Manage Automation of Its Trademark Operations*, GAO/IMTEC-85-8, Apr. 19, 1985, and testimony of Thomas P. Giammo before the Oct. 18, 1985 hearing of the Subcommittee on Government Information, House Government Operations Committee.

[33] See Mitch Betts, "Congress Steps Up Role in Federal Automation Projects," *Computerworld*, July 15, 1985; and statements of Guy Blynn of the U.S. Trademark Association and Herbert Wamsley of the Intellectual Property Owners, Inc., before the Oct. 1, 1985, hearing of the Subcommittee on Government Information, House Government Operations Committee.

[34] Office of Management and Budget, "Management of Federal Information Resources," *Federal Register*, vol. 50, No. 51, Mar. 15, 1985, Section 8(a)(8).

[35] Ibid., Section 8(a)(g). For further discussion, see Harold C. Relyea, Jane Bortnick, and Richard C. Ehlke, *Management of Federal Information Resources: A General Critique of the March 1985 OMB Draft Circular—Matters for Possible Congressional Consideration*, Congressional Research Service, Library of Congress, July 5, 1985.

[36] Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources," Dec. 12, 1985, Sections 7(a) and (b).

In sum, OMB appears to have tacitly acknowledged that aspects of the circular dealing with information dissemination do not have the clear congressional guidance originally assumed. Nonetheless, OMB has used its discretion and general authority to finalize the circular's emphasis on the private sector, even though Representative Glenn English, Chairman of the House Committee on Government Operations, Subcommittee on Government Information, among others, had requested that the draft circular be reconsidered.

Institutional Responsibility for Government Information Policy and Operations

The shifting of the Federal Government toward greater electronic information collection, maintenance, and dissemination appears to be further aggravating conflicts over the role of OMB, the Joint Committee on Printing, and GPO with respect to public information policymaking. It also is aggravating conflicts between OMB and various other congressional committees with respect to the applicability and interpretation of the Paperwork Reduction Act, and between GPO and NTIS and other Federal printing and electronic dissemination agencies over future operational responsibilities.

OMB has taken the position that electronic-based information dissemination by executive branch agencies falls outside of the definition of printing and binding in chapter 5 of Title 44 of the U.S. Code. In addition, the U.S. Department of Justice has interpreted the Supreme Court's decision in *INS* v. *Chadha*[39] (that struck down the legislative veto as unconstitutional) as invalidating parts of chapter 5 of Title 44 relating to the control of GPO over executive agency printing decisions. The printing chapters of Title 44 were originally enacted as the Public Printing Act of 1895 and were recodified in 1968 by Public Law 90-620. Prior efforts to enact a major revision to the printing chapters of Title 44 have not reached fruition. Thus, Title 44 has not yet been fully updated in light of modern information technology. Congress may wish to include this issue as part of a comprehensive review and revision of Federal public information policies.

The Paperwork Reduction Act of 1980 does provide clear congressional guidance, both in the language of the act and the legislative history, on the need to minimize the Federal paperwork collection burden, establish coordinated and uniform Federal information policies, and minimize the cost to the government of collecting, using, and disseminating information.[40]

At the same time, the act and its legislative history show that the need to maximize public access to government information was also intended by Congress. For example, the purpose of the act is, among other things, "to maximize the usefulness of information collected by the Federal Government,"[41] and the Senate report states that:

> The Committee expects the Director [of the Office of Information and Regulatory Affairs] to take appropriate steps to maximize public access to the information the Federal Government collects.[42]

The Federal Information Locater System, which the PRA of 1980 required OMB to establish, was also intended to help serve this purpose.[43]

---

[37] Ibid., Sections 9(a) and (b).

[38] Ibid., Sections 11(b) and (c).

[39] 103 S. Ct. 2764 (1983).

[40] 44 U.S.C. 3501 (1) and (2).

[41] 44 U.S.C. 3501 (3).

[42] S. Rep. No. 96-930, p. 33.

In addition, several new issues have arisen since enactment of the PRA in 1980. The congressional debate leading up to enactment of the PRA in 1980 did not consider many of the current issues, such as equity and private sector involvement in electronic systems, because these issues had not yet developed. Agency plans and practices for electronic government information systems reached threshold levels of visibility and significance only in the last few years. Also, the PRA debate, with a focus on government paperwork and information management, did not explicitly consider the numerous public laws that assign government information functions to numerous Federal agencies. In sum, PRA provides, at best, limited and mixed guidance to OMB with respect to the electronic collection, maintenance, and dissemination of government information. Congress may wish to update and clarify its intent with respect to the public information aspects of PRA through appropriate amendments and/or oversight and authorizing reports.

With respect to operational responsibilities for government information dissemination, historically GPO and national libraries have had a primary role. However, as a result of the increasing volume of government information—in many cases mandated by statute—coupled with the transition to electronic systems, NTIS and several of the agencies also have become major disseminators of government information. GPO, NTIS, the national libraries, and several agencies have developed numerous electronic and computer-based information products and services. For example, GPO makes the U.S. Code, Congressional Record, and Federal Register available in computer tape format to private publishers and information providers. Also, GPO makes its catalog to government publications available to depository libraries in an on-line electronic format.

And NTIS has expanded far beyond paper or microfiche copies of printed reports to include bibliographic, database, software, and related functions in cooperation with numerous other Federal agencies. These NTIS activities include, for example:

- *computer software*—more than 500 software programs, from more than 100 Federal agencies, available for purchase in magnetic computer tape format;
- *energy software*—more than 730 programs available for purchase in cooperation with the Department of Energy National Energy Software Center;
- *computerized data files*—about 1,000 data files are available in computer tape format;
- *floppy diskette files*—about 60 files available in diskette format (also, any computerized data file can be converted);
- *energy modeling programs*—about 55 computer modeling programs available on computer tape; and
- *other databases*—from the Defense Logistics Supply Center, Human Nutrition Information Service (USDA), and National Center for Health Statistics (DHHS).

In 1979 an advisory group appointed by the Joint Committee on Printing considered the possibility of establishing a new central office combining the functions of GPO, NTIS, and OMB with respect to public information policy, in order to facilitate public access and eliminate duplication. A National Publications Act of 1980 was introduced to establish a National Publications Office along with a commission that would replace the Joint Committee, but the bill was not enacted.[44]

---

[43] 44 U.S.C. 3501 (2)(B) and (D).

[44] See Levin, "Access and Dissemination Issues," op. cit., pp. 129-130; U.S. Congress, Joint Committee on Printing, Ad Hoc Advisory Committee on Revision of Title 44, *Federal Government Printing and Publishing: Policy Issues*, Washington, DC, 1979; and "National Publications Act of 1980," 96th Cong., 2d sess.

Public Information Index or Clearinghouse

Whether or not Congress establishes a centralized public information office, a centralized index to or clearinghouse of government information could be set up and operated by an existing or new entity. The library community has strongly advocated the need for such an index or clearinghouse, given the very large amount, numerous types, and many locations of government information.

One specific opportunity that has not been fully realized is the further development of the Federal Information Locater System (FILS) (or the equivalent) into a governmentwide electronic directory of public information products—both electronic- and paper-based. In enacting the Paperwork Reduction Act of 1980, Congress specifically required OMB to establish FILS and develop a proposal to augment it to include data profiles of all major agency information holdings.[45] The U.S. Senate report accompanying the act states that FILS is to:[46]

1. identify duplication in agencies' reporting and recordkeeping requirements;
2. locate existing information that may meet the needs of Congress, executive agencies, and the public; and
3. assist in deciding which agency requests for information collection should be approved.

FILS is now operational, but is designed and used primarily for #1 above, secondarily for #3, and not at all for #2. A National Bureau of Standards study (sponsored by OMB) of possible FILS improvements has been completed, but did not address objective #2.[47]

The further development of FILS or the equivalent should be able to build, to some extent, on the prior work of the many agencies that have a directory or catalog of their own public information products. Indeed, 67 out of 119 agencies (or 56 percent) responding to the OTA Federal Agency Data Request indicated the existence of a directory or catalog, and this included almost all of the largest public information providers (e.g., Census, NTIS, NCHS, Energy Information Administration (EIA), U.S. Geological Survey, and the National Institute of Justice).

The directories are mostly in a paper format, although some agencies also have or contract for computerized bibliographic services, and many agency reports and documents are indexed in various government and commercial on-line information retrieval systems. For example, GAO publishes a directory titled *Federal Information Sources and Systems* that is available in paper format and on the SCORPIO (Library of Congress) information retrieval system.[48] And a private publisher produces *The Computer Data and Database Source Book* in both hardcopy and electronic format (the latter via NewsNet).[49]

Mechanisms for Exchange of Learning and Innovation

Despite the activities of various individual Federal agencies, there appears to be no effective governmentwide mechanism to exchange learning and take advantage of the full range of innovative opportunities presented by information technology to facilitate access to and dissemination of public information.

The public information area appears to have received relatively little attention from the central agencies for information technology management—OMB, NBS, and GSA. There is little evidence of an organized effort to share experience and learning across agency lines, and to help derive the most benefit from agency experiments with and innovative applications of information technology for public information purposes. One or more of the central agencies could take on a larger role in this area, and/or some other agency or agencies whose primary mission is public information (e.g., the Bureau of Labor Statistics, EIA, GPO, NTIS) could be asked to serve as a focal point for the exchange of learning and innovation.

---

[45] Public Law 96-511; Section 3505 (2)(B) and (D).

[46] S. Rep. No. 96-930, p. 2.

[47] U.S. Department of Commerce, National Bureau of Standards, *Recommendations for the Improvement of the Federal Information Locator System*, October 1984.

[48] U.S. Comptroller General, *Federal Information Sources and Systems 1984*, GAO/AFMD-85-3, General Accounting Office.

[49] Matthew Lesko, *The Computer Data and Database Source Book* (New York: Avon, 1984).

Several examples of agency innovation have been cited previously. Two others include TradeNet and the Microcomputer Electronic Information Exchange. TradeNet is a computer-based electronic network that includes databases, analytic software, electronic mail, and other automated capabilities with respect to information relevant to international trade policy. Several agencies (e.g., the Office of the U.S. Trade Representative; Departments of Agriculture, Commerce, and Labor) pooled resources to develop a more accurate and timely information base on trade policy—drawing from U.S. Government, international, and private sector sources. TradeNet's central files are maintained at the National Institutes of Health computer center, and files are accessed electronically in real-time or by downloading to mini- and micro-computers.[50] Another approach is the electronic bulletin board, illustrated by the Microcomputer Electronic Information Exchange, operated by NBS. This is a public bulletin board that provides information on microcomputer: courses, access to other bulletin boards, user groups and meetings, security products and issues, and technical information, among other topics.[51]

Some technological opportunities that do not, as yet, appear to be receiving very much governmentwide attention include: remote electronic printing and printing-on-demand for dissemination of government reports to the public; computer-assisted surveys and data collection for statistical purposes; videotex (or the equivalent) information systems networked with depository and public libraries; and microcomputer-based systems for individual access to the major public information databases.

The Canadian Government's nationwide videotex-based public information system is one example of what is technically feasible. More than 2,000 videotex terminals have been located in government agencies, libraries, and other public places. A wide variety of information is available—ranging from a nationwide job bank, weather forecasts, and national park services to the status of bills in Parliament. The public has free access at public buildings (e.g., libraries, post offices), and can, for a fee, gain access via personal computers.[52] Another example is a recently launched European electronic publishing program that is aimed at providing a complete service for the electronic storage, transmission, and delivery of documents. This program is being run by a group of publishers, software houses, computer service bureaus, and governmental entities. Technologies include user-friendly videotex, digital optical disks, high-speed telecopy, and satellite transmission.[53]

Freedom of Information Act Implementation

OTA found that very few Federal agencies are directly using information technology to facilitate the processing of FOIA requests, and the results of these few applications are not being effectively shared. Possible opportunities for innovation are neither being studied nor tested.

The response to the OTA Federal Agency Data Request indicated that few agencies receive or respond to FOIA requests in electronic form. A handful of agencies are just beginning to consider the possibilities, although only one agency (the Federal Aviation Administration) reported a completed, ongoing, or planned formal study on this topic.

---

[50] Harry Goldberg, "TradeNet: Enhanced Accuracy & Economy Result From Interagency Data Pooling," *Government Executive*, vol. 17, No. 1, January 1985.

[51] For more information, the dial-up number is (301) 948-5718 (ASCII, 1200 baud, 8 or 7 data bits, even or no parity, 1 stopbit).

[52] "Canada Sets Pace in Making Government Accessible to All," *Government Executive*, February 1985, pp. 37-41.

[53] "European Electronic Publishing Program," *Information Hotline*, February 1985, p. 4. See also, for discussion of proposals for U.S. innovations, National Commission on Libraries and Information Science and U.S. Department of Agriculture, *Joint Congressional Hearing on the Changing Information Needs of Rural America: The Role of Libraries and Information Technology*, July 21, 1982; National Commission on Libraries and Information Science, *Community Information and Referral Services*, May 1983; and U.S. Congress, Joint Committee on Printing, *Provision of Federal Government Publications in Electronic Format to Depository Libraries*, 98th Cong., 2d sess., 1984.

Some agencies are using computerized systems to improve the internal tracking and processing of FOIA requests, with apparently good results. Other agencies recognize that computerized records can, in general, speed up processing time. However, these positive experiences do not appear to be shared effectively with other agencies.

Beyond this, however, several States appear to be ahead of the Federal Government in their consideration of electronic public access to government information. For example, the State of California commissioned a study on electronic public access that concluded that:

> The opportunities [of direct electronic access] revolve around the possibility of making government—particularly the records of government—more readily accessible to the people of California. On-line inquiry, when coupled with powerful computerized file search capabilities, creates the possibility of employing public information as a true public resource, accessible to a much larger segment of the population than was possible in the past.[54]

However, the study also identified a number of issues that needed resolution, including: 1) meeting the public's right to know while protecting the individual's right to privacy, 2) ensuring the proprietary rights of individuals and commercial enterprises, 3) providing adequate security, and 4) establishing fair and equitable prices.

A similar study was conducted by the Florida State Legislature's Joint Committee on Information Technology Resources. This study examined a wide range of issues raised by proposals to permit direct computer access to public records. The Joint Committee found that the majority of Florida's State public record systems had been automated, and recommended, among other things, that:

- remote electronic access to automated information systems maintained by public record custodians should be authorized by statute and encouraged as a matter of public policy;
- a pilot project demonstrating remote electronic access to State automated records should be undertaken;
- public record custodians should be allowed to charge for costs of computer time in fulfilling requests for copies of public records, but only after uniform cost methodologies are established in statute and rules; and
- access to all State data systems should be made available to elected members of the Florida Legislature.[55]

Florida's analysis, as did California's, recognized the need to consider Privacy and Public Records (or Freedom of Information) laws; security, training, and cost recovery issues; technical concerns; responsibility for record quality and archiving; and the broader implications for citizen participation in government when formulating policy on electronic access.

An emerging issue identified in OTA's review of innovative activities in selected States (Michigan, Virginia, Oregon, and North Carolina, in addition to California and Florida) is the extent to which public records or databases, when computerized in an on-line format, become legally accessible to the public—regardless of whether or not such information is already provided by private vendors. For example, public access advocates argue that once government agencies computerize information on scheduling of public meetings and hearings, minutes and proceedings resulting from public activities, current status of regulatory and legislative initiatives, and the like, this electronic information should be accessible to the public—at little or no cost.[56]

---

[54] State of California, Department of Finance, Office of Information Technology, "Accessing California State Data Bases: A Preface to 'Framework to Develop Computer Information Public Access Policy,' " Dec. 26, 1984; see generally, Touche Ross & Co. and EDP Audit Controls, Inc., *Framework To Develop Computer Information Public Access Policy*, prepared for the Office of Information Technology, California State Department of Finance, Jan. 1, 1985.

[55] State of Florida, Legislature, Joint Committee on Information Technology Resources, *Remote Computer Access to Public Records in Florida*, January 1985. Also see Donna Raimondi, "Florida Bill Proposes Electronic Access Into Agencies," *Computerworld*, Apr. 1, 1985, p. 19.

The selected State review (plus a review of activities in selected localities—Lane County, Oregon; Columbus, Ohio; and Beverly Hills, Irvine, Palos Verdes, and Buena Park, California) concluded that the two information technology applications with the greatest real potential for facilitating public access are:

1. electronic access to information about the process and results of government activities, especially decisionmaking activities; and
2. access to the databases and computer models used by government agencies to formulate positions on various sides of the issues.[57]

The review identified a wide range of technical options—from cable television and videotex to microcomputer access over electronic data networks—but concluded on a note of caution. Many past expectations about using information technology to facilitate public access have not been met—sometimes due to lack of citizen interest and sometimes because the groups using the new electronic options are those that already have the resources and sophistication to get access now, among other factors. In sum, information technology appears to offer significant potential to facilitate implementation of public records and freedom of information laws—whether at the Federal, State, or local levels. But realizing this potential depends in large part on an interested and educated citizenry and the absence of any significant technical or cost barriers.[58]

Electronic Recordkeeping and Archiving

The growing use of information technology in the creation and maintenance of Federal records could have a profound effect on the recorded history of Federal programs and decisions, and thus could affect the record base subject to the FOIA in particular and public access in general. If key Federal records were electronically erased or destroyed, the FOIA and public access mechanisms, however strong, would be undermined.

The increase in computerized files, but most significantly the explosion in microcomputer and word processing terminals, means that record creation and recordkeeping have been decentralized. File clerks and secretaries no longer have clear physical control over records management. Agency staff who use word processing software are able to create, manipulate, file, review, delete, and communicate documents. If those documents meet the definition of Federal records, then legally these records should be retained to preserve the documentation for different steps in the decisionmaking process.

Record managers, researchers, historians, and archivists are properly concerned that key Federal records may be lost, altered, or destroyed by agency staff who do not understand Federal record management requirements. The National Archives and Records Administration (NARA), GSA, and Senate Historical Office, among others, have pointed out the need to develop educational, training, technical, and policy strategies to deal with this potential problem. These agencies have emphasized that now is the time to address these questions while Federal agencies and employees are still learning about, and developing policies and procedures for, microcomputer use.

---

[56] See generally Kenneth L. Kraemer, John Leslie King, and David G. Schetter, *Innovative Use of Information Technology in Facilitating Public Access to Agency Decisionmaking: An Assessment of the Experience in State and Local Governments*, OTA contractor report, March 1985.

[57] Ibid., pp. 44-49.

[58] Ibid.; also see, for example, Bruce Gates, "Knowledge, Networks, and Neighborhoods: Will Microcomputers Make Us Better Citizens?" *Public Administration Review*, March 1984, pp. 164-169; and William Dutton, et al., "Electronic Participation by Citizens in U.S. Local Government," *Information Age*, April 1984, pp. 78-97. For some of the earliest work on this topic, see John D.C. Little, Thomas B. Sheridan, Chandler H. Stevens, and Peter Tropp, *Citizen Feedback Components and Systems* (Cambridge, MA: MIT, June 1972); Norman Johnson and Edward Ward, "Citizen Information Systems: Using Technology To Extend the Dialogue Between Citizens and Their Government," *Management Science*, December 1972, pp. p-21 to p-34; Chandler Harrison Stevens, Floyd E. Barwig, Jr., and David S. Haviland, *Feedback: An Involvement Primer* (Troy, NY: Rensselaer Polytechnic Institute, January 1974); Roy Amara, *Toward Understanding the Social Impact of Computers* (Menlo Park, CA: Institute for the Future, May 1974); and Fred B. Wood, "Congressional-Constituent Telecommunication: The Potential and Limitations of Emergent Channels," *IEEE Transactions on Communications*, vol. 23, No. 10, October 1975, pp. 1134-1142.

As a result, NARA and GSA recently issued preliminary guidelines for agencies regarding electronic recordkeeping, and have initiated major projects to further research the records management problems presented by the creation, maintenance, use, and disposition of electronic records. The wide scope of concern is illustrated by the topics covered in the preliminary bulletin:

- electronic records creation practices,
- indexing electronic records,
- retrieval of electronically stored records,
- ensuring the retention of electronic records,
- destruction of electronic records,
- electronic record standards,
- judicial use of electronic records,
- appropriate electronic records storage medium,
- electronic records security,
- software for electronic record systems,
- equipment configuration for electronic record systems, and
- flexible disk care and handling for electronic records.[59]

The magnitude of the problem is reflected in the following statement by a senior NARA official in explaining why and how the government could lose a significant portion of its institutional memory:

> The impact of automation is broad ranging. Program and policy officials, sitting at their terminals, decide the fate of the information they create and receive, while in the past people trained in records management made these decisions. With the use of paper, the development of policies was simple to trace. Successive drafts indicated the evolution of decisions. With computers, though, drafts no longer exist. Instead, policy papers evolve and each new version is written over the previous one. With paper files, most people appreciated the need for a coherent, centralized filing system. The increased use of automation masks this need and individuals develop personalized retrieval systems, many of which would be incomprehensible to anyone else.[60]

Finally, the Acting Archivist of the United States has raised a serious concern that electronic recordkeeping may undermine aspects of the Privacy Act with respect to the currency and accuracy of Privacy Act records and their disposition. For example, electronic records may be destroyed too quickly before the record subject can, if he or she desires, check the record quality, or may be retained too long, and become stale and outdated. The Archivist believes that, while most records officers now agree that electronic records are fully subject to the Federal Records Act and other relevant public laws, many records managers need additional training and motivation—as well as guidance—in order to develop appropriate electronic records management programs.[61]

In sum, leading government historians and archivists believe that the United States is in danger of losing its memory, "and that historically significant first drafts of key policy documents may be lost." Thus "[b]ecause of erasures of electronic records, future historians may know less about the 1985 arms control talks than about the 1972 Strategic Arms Limitations Talks."[62]

Scientific and Technical Information

Scientific and technical information (STI) collected and/or developed at Federal Government expense is an important subset of all government information. The role of information technology has aggravated some old issues and raised some new ones. On the positive side, electronic STI systems have now become a significant, if not indispensable, part of the scientific research and engineering enterprise in the United States and other technologically advanced nations. Computerized bibliographic and information retrieval systems are commonplace, as are various forms of computer networking—up to and including supercomputer networks. The use of electronic mail, electronic bulletin boards, and computer-conferencing is growing, although still at very modest levels. These technologies present further opportunities for innovation.[63]

---

[59] U.S. General Services Administration, FIRMR Bulletin 23 on "Electronic Recordkeeping," June 18, 1985.

[60] Patricia Aronsson, Director, NARA Documentation Standards Division, letter to Fred Wood of OTA, Apr. 9, 1985.

[61] Frank G. Burke, Acting Archivist of the United States, letter to Fred Wood of OTA, Oct. 4, 1985.

[62] Mitch Betts, "Federal Historians Alarmed at Loss of Computerized Data," *Computerworld*, Sept. 23, 1985, p. 34.

On the negative side, the U.S. science and engineering community appears to be so dependent on information technology to retain a competitive edge that any reductions (or even reduced growth) in this technological support are viewed with serious concern, especially in the university research community. The issues discussed earlier with respect to public information generally (e.g., greater emphasis on private sector commercial offerings and full cost recovery) may actually be even more salient in the university research community, in part because of the high percentage of Federal financial support for university research and development.[64]

Commercialization of scientific and technical data is a continuing issue. A strongly held view in the scientific community is that the best research results from full and open communication and easy availability of the latest data and research findings. A good example is the debate over the Landsat Earth remote-sensing satellite program. Congress ultimately decided to transfer this program to the private sector for commercial development, over the objections of some researchers who felt that this valuable source of data might be priced out of reach if placed in a private firm.[65] This same concern has been expressed about a number of STI systems, such as the Environmental Protection Agency's transfer of its chemical information system (known as CIS) to private vendors.[66]

Overall, all of the trends, issues, and opportunities discussed previously with respect to public information generally appear to apply to STI, with the further complicating factor of national security. Classified information is, of course, exempted from disclosure under FOIA and is not public information. The problem with STI is striking the appropriate balance between adequate protection for sensitive STI, on the one hand, and open and broad dissemination of STI among the research community, on the other. This involves, in part, concern about overclassification, but more importantly that unclassified STI may be restricted due to its possible use in ways that could affect national security. The tensions between open scientific exchange and tight military control of STI have heightened in recent years, in part because of information technology and the vastly increased speed, content, and complexity of electronic STI networks. Numerous professional and technical organizations have heavily resisted DOD efforts to curtail the exchange of STI. This issue is likely to continue for the foreseeable future.[67]

---

[63] See Jane Bortnick and Nancy Miller, *The Impact of Information Technology on Science*, Congressional Research Service, Library of Congress, July 1985, especially sections II and III; and, generally, U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues*, OTA-CIT-268 (Washington, DC: U.S. Government Printing Office, February 1985). For a detailed discussion of one Federal agency's technical information activities, see U.S. Department of Energy, Office of Scientific and Technical Information, "Technical Information Management Activities: What They Are and How They Relate to and Support the DOE R&D Programs" (Oak Ridge, TN: August 1985).

[64] See Bortnick and Miller, *Information Technology*, op. cit., esp. pp. 39-41, 57-60; and Patricia Battin, "Problem Trends in the Information Marketplace," *Chronicle of International Communication*, September-October 1985, pp. 5-6.

[65] Ibid.; U.S. National Commission on Libraries and Information Science, *Information Policy Implications of Archiving Satellite Data: To Preserve the Sense of Earth From Space*, Washington, DC, 1984; and U.S. Congress, Office of Technology Assessment, *Remote Sensing and the Private Sector: Issues for Discussion—A Technical Memorandum*, OTA-TM-ISC-20 (Washington, DC: U.S. Government Printing Office, March 1984). Also see statements of witnesses at Nov. 13, 1985, hearing on "Oversight of Landsat Commercialization," held by the U.S. Senate, Committee on Commerce, Science and Transportation, Subcommittee on Science, Technology, and Space.

[66] Jeffrey L. Fox, "EPA Dumps Chemical Data System" *Science*, vol. 226, November 1984, p. 816.

[67] See Bortnick and Miller, *Information Technology*, op. cit., pp. 57-60; also Mitchel B. Wallerstein, "Scientific Communication and National Security in 1984," *Science*, vol. 224, May 4, 1984, pp. 460-466; Harold C. Relyea, "National Security Controls and Scientific Information," Congressional Research Service, Library of Congress, Issue Brief 82083, Sept. 11, 1984; Robert L. Park, "Restrictions on Scientific Freedom," *IEEE*

(continued on next page)

Other Issues

OTA identified four other issues that warrant attention. These are described briefly below:

1. *Transborder information flow.* Variations in national laws and policies on information may restrict the free flow of information between nations, and curtail international market opportunities for U.S. firms. On the other hand, information technology permits a vastly expanded range of technical options for international (or transborder) information flow.[68]
2. *Depository library system.* The depository library system is viewed by some as part of the public information "lifeline" or "safety net" to ensure that the public has at least one avenue of unrestricted access. Some researchers have questioned how much government information actually gets into the depository libraries, and to what extent the public is aware of and uses the libraries. Modern electronic information technologies are already important to the depository system, and are opening up many new opportunities.[69]
3. *Federal statistical system.* Federal statistical agencies are among the major Federal Government public information providers; their activities are relevant to all of the issues previously discussed. However, the statistical community has, over the last 5 years, raised questions about the proper development and coordination of Federal statistical policy, the impact of budgetary cuts and restrictions, and the appropriate role of electronic technology in the collection, maintenance, and dissemination of statistical information.[70]
4. *Copyright protection.* Although copyright law prohibits the copyrighting of government information developed directly by government agencies, there continues to be concern about the status of information developed by government contractors, for example, those conducting research and development. Also, the legality and propriety of Federal agencies giving private vendors exclusive control over or rights to agency information have been questioned, as has the implicit control resulting from exclusionary pricing (e.g., pricing at a level that only trade associations, law firms, and business can afford and not most individual citizens, researchers, and public interest groups). It is not clear whether technology is part of the problem, part of the solution, or both.[71]

Technology and Society Magazine, March 1985, pp. 7-9; Eric J. Lerner, "DOD Information Curbs Spread Fear and Confusion," *Aerospace*, March 1985, pp. 76-80; and "Societies Warn Defense Department of 'Counterproductive' Information Controls," *The IEEE Institute*, November 1985, pp. 1, 4.

[68] See, for example, LINK Resources Corp. and Transnational Data Reporting Service, Inc., *Strategic Response to Regulation of Transnational Data Flows*, New York, 1979.

[69] See U.S. Congress, Joint Committee on Printing, *Provision of Federal Government Publications in Electronic Format to Depository Libraries*, report of the Ad Hoc Committee on Depository Library Access to Federal Automated Data Bases, Washington, DC, 1984; Peter Hernon, "Provision of Federal Government Publications in Electronic Format to Depository Libraries," *Government Information Quarterly*, vol. 2, No. 3, 1985; pp. 231-234; U.S. Congress, Joint Committee on Printing, *An Open Forum on the Provision of Electronic Federal Information to Repository Libraries*, Report of the Committee Staff, 99th Cong., 1st sess., June 26, 1985; and Sarah Kadec, "The U.S. Government Printing Office's Library Program's Service and Automation: An Insider's Commentary," *Government Publications Review*, vol. 12, 1985, pp. 283-288.

See U.S. General Accounting Office, *Status of the Statistical Community After Sustaining Budget Reductions*, GAO IMTEC-84-17, July 18, 1984; U.S. Congress, House Committee on Government Operations, *The Federal Statistical System, 1980 to 1984*, 98th Cong., 2d sess., a report prepared by Baseline Data Corp. for the Congressional Research Service, November 1984; and U.S. Congress, House Committee on Government Operations, *An Update of the Status of Major Federal Statistical Agencies, Fiscal Year 1986*, 99th Cong., 1st sess., May 1985.

For general discussion of copyright and other intellectual property issues, see OTA, *Intellectual Property Rights in an Age of Electronics and Information*, forthcoming in late 1986.

Chapter 8

Information Technology and Congressional Oversight

Contents

Page
Summary 161

Introduction 162

Current Status of Information Technology in Congress 163

Oversight Opportunities 164
  Access to Agency Electronic Files 165
  Computer-Based Modeling and Decision Support 167
  Video- and Computer-Conferencing 169
  Electronic Tracking of Agency and Executive Actions 171

Chapter 8

Information Technology and Congressional Oversight

SUMMARY

The preceding chapters of this report focus primarily on management, use, and congressional oversight of information technology in the executive branch. The trends, issues, and options discussed are properly within the purview of congressional oversight of executive branch programs, activities, and implementation of public laws. However, information technology also has a potential role in the actual conduct of congressional oversight.

Over the last 10 to 15 years, Congress as a whole has made great strides in using information technology with respect to legislative information retrieval, constituent mail, correspondence management, and some administrative functions. For example, Members of Congress and congressional staff now have access to a wide range of computer-based services, such as computerized tracking of current bills and amendments; and computerized bibliographic databases and legal information retrieval systems, some operated by Congress and others by private vendors. There are now several thousand computer terminals in Congress, compared to only a handful in 1970. Also, both the House and Senate now have well-developed information technology support offices.

However, the use of information technology for direct support of congressional policymaking and oversight is just beginning. A similar situation exists at the State level, based on an OTA review of relevant activities in nine State legislatures (California, New York, Wisconsin, Minnesota, Florida, Washington, Texas, Virginia, and South Dakota). The development of legislative information technology appears to follow a common pattern where policymaking and oversight applications follow, rather than lead, basic administrative, correspondence, and information retrieval applications.

OTA identified significant unrealized opportunities for congressional use of information technology in conducting oversight, and an apparent lack of clear strategy for such use. Four specific opportunities identified by OTA include: 1) direct access by congressional committees and staff to agency electronic files and databases, 2) use of computer-based modeling and decision support, 3) video- and computer-conferencing to augment committee and staff oversight activities, and 4) electronic tracking of agency and executive actions. Congress may wish to plan and conduct a series of pilot tests and demonstrations in each of these areas in order to more accurately assess the benefits, costs, and problems.

The pilot test approach has worked in the past for new technological applications in Congress. Pilot tests of congressional oversight applications should be useful to help familiarize Members and staff with new applications, identify needs for training, and develop the best match or fit between a particular application and the needs of specific committees, Members, and staff. Also, while Congress has strong constitutional powers to oversee and obtain information from the executive branch, pilot tests would help familiarize the agencies with new applications, identify any needed adjustments, and generally seek approaches that minimize possible concerns about separation of powers and executive privilege.

Numerous alternatives for implementing pilot tests are available to Congress, ranging all the way from accessing carefully selected agency databases in specific subject areas; to requesting that selected agency submissions

to Congress be presented in a decision analytic framework; to running—on a trial basis—illustrative agency decision support models with alternative assumptions and data; to establishing a pilot congressional "situation room" for oversight purposes. Several of the options discussed previously in chapters 6 and 7 could also be helpful in the use of information technology for congressional oversight, such as guidelines on model evaluation, procedures for monitoring and exchanging key trends information, and directories or indices to major databases and computer models.

INTRODUCTION

Previous chapters of this report have focused primarily on the management and use of information technology by the executive branch of the Federal Government, and in particular those trends, applications, opportunities, and issues that warrant congressional attention. The prior chapters deal largely with appropriate substantive topics for congressional oversight of Federal Government information technology. This chapter deals with the use of information technology in the process of conducting congressional oversight.

Congressional applications of information technology span the spectrum from correspondence management and computerized mail, to electronic voting, to computerized bibliographic searches and information retrieval. Congressional use of information technology can have implications in a variety of areas—ranging from the efficiency, working conditions, and organizational structure of Congress; to the legislative, investigative, and constituent service functions of Congress; to the political effectiveness of Congress in representing the diverse interests of this Nation; and, finally, to the quality of the public policymaking process and the power of Congress relative to other branches and levels of government.[1]

This chapter focuses on only a few aspects of congressional use of information technology—specifically, the current and potential use of information technology in conducting congressional oversight of executive branch programs, activities, and implementation of public laws, as well as oversight of general societal trends and issues that are relevant to the legislative process.

This chapter first presents a brief review of the current status of information technology in Congress; and then discusses several unrealized opportunities for congressional use of information technology in conducting oversight of executive branch agencies, programs, and activities.

For further discussion, see Stephen E. Frantzich, "Congressional Applications of Information Technology," OTA contractor report, February 1985; Robert L. Chartrand and Trudie A. Punaro, *The Legislator As User of Information Technology*, Congressional Research Service, Library of Congress, Report No. 84-170 S, Dec. 7, 1984; and Stephen E. Frantzich, *Computers in Congress: The Politics of Information* (Beverly Hills, CA: Sage Publications, 1982). Also see Rex V. Brown, "A Brief Review of Executive Agency Uses of Personalized Decision Analysis and Support," OTA contractor report, Mar. 14, 1985; and Rex V. Brown, "Decision Analysis As a Tool of Congress," OTA contractor report, May 10, 1985.

CURRENT STATUS OF INFORMATION TECHNOLOGY IN CONGRESS

Members of Congress and congressional staff now have access to a wide range of computer-based services, such as:[2]

- major issue briefs prepared by the Congressional Research Service (CRS) and available in on-line electronic format, on microfiche, in hard copy, and, selectively, on audiocassettes;
- legislative information systems that allow computerized tracking of current bills and amendments by subject, sponsor, and number;
- computerized bibliographic databases such as SCORPIO (operated by the Library of Congress), which includes, for example, legislative history information and *Congressional Record* abstracts, and DIALOG (a commercial service operated by Lockheed), which provides access to numerous public and private databases; and
- computerized legal information retrieval systems, such as LEXIS (a commercial service operated by Mead Data Central), which contains the U.S. Code and Supreme Court and State Court decisions, and, where necessary, JURIS (Justice Retrieval and Inquiry System, operated by the U.S. Department of Justice) and FLITE (Federal Legal Information Through Electronics, operated by the U.S. Department of the Air Force).

In addition, Congress makes extensive use of computerized mail, correspondence management, scheduling, and administrative systems, use of electronic voting and televised floor proceedings (House only), and some use of electronic mail and computer-based decision support. Many congressional scholars now believe that Congress has, indeed, moved into the information age. Political scientist Stephen E. Frantzich, of the U.S. Naval Academy, in a 1985 paper on "Congressional Applications of Information Technology" prepared for the Office of Technology Assessment, observes that:

> A decade ago, Congress stood in the backwaters of information technology applications with little more than routine payroll uses of the computer. Congress' timidity to enter the "Information Age" has been replaced by an aggressive desire to provide both the institution and its individual members with the sophisticated information tools available in other realms.

Both the House and Senate have developed information support offices that provide a wide range of services and in-house consulting to Members and staffs. These responsibilities have been assigned in the House to the House Information Systems Office (HIS, with oversight by the House Administration Committee) and in the Senate to the Senate Computer Center (operated by the Senate Sergeant of Arms with oversight by the Senate Rules and Administration Committee). Both HIS and the Senate Computer Center provide general technical assistance to Congress in such areas as:

- designing and computerized processing of surveys;
- facilitating access to econometric models;
- developing custom computer models;
- accessing computerized demographic and geographic data;
- developing computer-assisted graphics for organizing and presenting information;

---

[2] Frantzich, "Congressional Applications," op. cit.; and Chartrand and Punaro, *The Legislator*, op. cit.

- using electronic spreadsheets and other computer software; and
- accessing computerized statistical, budget, and programmatic data.[3]

In general, HIS and the Senate Computer Center make their technical expertise available to assist congressional committees in analyzing data needs; obtaining and utilizing data; directly accessing computer systems for processing the data; and auditing and evaluating external computer systems and programs.[4]

Two other indicators document the movement of Congress into the computer age. There are now an estimated 7,500 computer terminals in Congress, compared to only a handful in 1970.[5] And the fiscal year 1983 legislative branch computer budget was about $73 million ($29 million for the House and Senate combined, the rest for congressional support offices),[6] compared to about $5 million in fiscal 1970 (about $0.7 million for the House and Senate combined).

Overall, modern information technology has become an indispensable part of the infrastructure of Congress with respect to legislative, administrative, and constituent service functions. However, the use of information technology for direct support of policymaking and oversight is only just beginning. As noted by Robert L. Chartrand of CRS:

> The development of legislative information technology has followed a clear pattern. In almost every instance, the initial applications support legislative and internal administrative functions, such as voting, bill status, bill drafting and code revision, committee calendars, payrolls, office accounts and correspondence. Only after these initial systems have been successfully implemented do most legislatures develop decision-making assisting and policy analysis applications.[7]

The available evidence suggests that Congress is now roughly on a par with the State legislatures with respect to basic applications of information technology. A 1984 survey of State legislatures (conducted by the National Conference of State Legislatures) found that 40 of 44 State legislatures responding had a computer system. States reported the following kinds of legislative applications: word processing (37 States); budget tracking (30); bill tracking (27); spreadsheet (23); graphics (22); editing (15); and audit tracking (7).[8]

---

[3] U.S. Library of Congress, Congressional Research Service, *Congressional Oversight Manual*, February 1984, pp. 104-107.

[4] Ibid.

[5] Steve Blakely, "Computers Alter Way Congress Does Business," *Congressional Quarterly*, July 13, 1985, pp. 1379-1382.

[6] Chartrand and Punaro, *The Legislator*, op. cit., p. 16.

[7] Frantzich, "Congressional Applications," op. cit., p. 69.

[8] Dale Nesbury, "Legislative Fiscal Office Computer Survey," National Conference of State Legislatures, Fiscal Affairs Program, July 12, 1984.

OVERSIGHT OPPORTUNITIES

OTA identified several specific opportunities for congressional use of information technology for oversight purposes, and an apparent lack of a clear strategy for such use. A similar situation exists at the State level, based on a review of relevant activities in nine State legislatures (California, New York, Wisconsin, Minnesota, Florida, Washington, Texas, Virginia, and South Dakota).[9] Despite scattered examples of innovation, the selected State review concluded that:

> [W]e certainly cannot say there is anywhere a thoughtful [State] legislative masterplan for greater oversight, augmented by the most modern means of information processing. Information technology has not been seized by the [State legislative] leadership as a major weapon in the ongoing struggle with the executive branch.[10]

---

[9] Robert Miewald, Keith Mueller, and Robert Sittig, "State Legislature Use of Information Technology in Oversight," OTA contractor report, January 1985.

[10] Ibid., p. 65.

In Congress, there is already an awareness of the oversight potential of information technology on the part of some staff and various Members who are among the leaders in using information technology.[11] And in some subject areas, primarily budget analysis, the congressional use of electronic databases and computer modeling for oversight purposes is significant.[12] But there appears to be no overall strategy or plan for congressional use of information technology for oversight.

Four specific opportunities were identified by OTA: 1) access to agency electronic files; 2) computer-based modeling and decision support; 3) video- and computer-conferencing; and 4) electronic tracking of agency and executive actions. Some pilot test possibilities are discussed below.

The discussion assumes that pilot tests and demonstrations would be conducted prior to full-scale implementation, in order to more accurately assess the benefits, costs, and problems. The pilot test approach seems warranted in view of the potential sensitivities of both the overseers (committee members and staffs) and the subjects of oversight (primarily executive branch agencies, programs, and officials, for purposes of this chapter). While Congress seems increasingly open to new applications of information technology, such applications need to be developed in ways that are compatible with the larger congressional process (e.g., hearings, investigations, legislative drafting) and with the skills and experience of Members and staff. Pilot tests would help familiarize members and staff with new applications, identify any needs for training, and work out the best match or fit between a particular application and the needs of specific committees, members, and staff. As for the executive branch agencies, while Congress has strong constitutional powers to oversee and obtain information from the agencies, some agency resistance and concern should be anticipated. Pilot tests would help familiarize the agencies with new applications, identify any needed adjustments or modifications, and generally seek approaches that minimize possible concerns about separation of powers, executive privilege, and congressional micromanagement.

Also, the following discussion assumes that pilot tests would be preceded by some kind of preliminary study, and that the primary technical support for pilot tests would be provided by the Senate Computer Center and House Information Systems staff, augmented where necessary by appropriate congressional committee and/or congressional support office staff. Actually, a useful early activity might be to develop a roster of interested congressional staff and their relevant skills. These staff could then be drawn on as possible participants in and/or advisors or consultants to various pilot projects of interest.

Access to Agency Electronic Files

A central aspect of congressional oversight is access to and review of information relevant to agency implementation of public laws and programs. Congress has always sought oversight information from the executive branch, and the constitutional power of Congress to obtain such information has, with few exceptions, been upheld by the courts:

- Indeed, "it is clear that official congressional committee requests for information are not subject to the disclosure restrictions of the FOI/PA [Freedom of Information Act/Privacy Act]."[13]
- And more generally, "[a] broad power to investigate and oversee the execution of the laws has also been inferred from the constitutional grant of legislative power to the Congress."[14]

---

[11] See Blakely, "Computers Alter," op. cit. Also see Edward Segal, "Computerizing Congress," *PC World*, November 1985, pp. 144-151.

[12] Use of computer-based budget and economic analyses appears to be concentrated in the Congressional Budget Office and House and Senate Budget Committees and in the Joint Committee on Taxation (which primarily serves the needs of the Senate Finance and House Ways and Means Committees).

[13] Freedom of Information Act, 5 U.S.C. 552(c), and Privacy Act, 5 U.S.C. 552a(b)(9). See Richard Ehlke, *Congressional Access to Information: Selected Problems and Issues*, Congressional Research Service, Library of Congress, Report No. 79-220 A, p. 38.

[14] Ehlke, Ibid., p. 28.

- The Supreme Court has held that "the power to investigate is inherent in the power to make laws because '[a] legislative body cannot legislate wisely or effectively in the absence of information respecting the conditions which the legislation is intended to effect or change.' "[15]

Nonetheless, congressional requests for agency information are frequently met with delays and resistance. A key question is whether information technology can help improve congressional access. This OTA study has documented elsewhere that a high percentage of agency files and record systems are now maintained in computerized form (see chs. 2 and 7 of this report and ch. 2 of OTA's *Electronic Record Systems and Individual Privacy*, forthcoming 1986). In theory, then, it should be quicker and easier for agencies to supply requested information in electronic rather than paper form, since all that would be necessary is making available a duplicate computer tape. Once received by Congress, the data on the computer tape could then be manipulated and analyzed to meet the particular needs of the congressional committees involved.

This possibility has been borne out in at least two cases—one congressional application and one press application. The first is the transmittal of the President's budget on computer tape from the Office of Management and Budget (OMB) to the Congressional Budget Office (CBO). This has permitted CBO to begin its budget analyses sooner and prepare reports for Congress on a more timely basis.[16] A second case, demonstrated by a former congressional staff person who is now an investigative reporter for Knight-Ridder Newspapers, is access to computer tapes of agency data—in this case, data maintained by the Bureau of Motor Carrier Safety (BMCS, a part of the Federal Highway Administration) on truck accident reports and safety investigations.[17] Here, the reporter filed a Freedom of Information Act (FOIA) request for copies of the agency's accident reports and safety inspections, but asked that the records be provided on computer tape rather than on paper. The agency provided the requested records in computer format within 2 weeks, according to the reporter, much faster than the usual FOIA response time of several months or longer for requests of this large size. In addition, the agency was easily able to delete the names of truck drivers from the records, on the grounds of confidentiality, an exercise that would have been very time-consuming if done with paper records. Over 400,000 documents were provided in electronic form and then analyzed using standard statistical software. The results provided key input to a series of articles on the BMCS's implementation of truck safety regulations and programs.[18]

Congressional requests for computerized agency records such as these are not subject to the FOIA. And, in general, the form of the record—whether paper or electronic—should make no difference with respect to the inherent congressional power to investigate and seek and obtain agency information.[19] Of course, agencies may resist anyway, as has happened on the State level in Vermont when the State legislature sought access to the executive branch computerized financial accounting system.[20]

A logical first step would be for participating congressional committees to review Federal agencies and programs within their jurisdiction and identify key types of information that are not presently available but would be useful to have in conducting oversight. The committees could then ask agencies whether they have the desired information and, if so, whether the information is computerized.

---

[15] Ibid., p. 29, which cites *Eastland v. United States Servicemen's Fund*, 421 U.S. 491, 504(1975), quoting *McGrain v. Dougherty*, 273 U.S. 135, 175(1927). Also see *Nixon v. Administrator of General Services*, 433 U.S. 425(1977).

[16] Frantzich, "Congressional Applications," op. cit., p. 56, citing Robert Harris of the Congressional Budget Office.

[17] Thomas J. Moore, Knight-Ridder Newspapers, telephone interview, Oct. 25, 1985.

[18] Ibid., and see four-part series on "Deadly Transport: The Perils of Interstate Trucking" by Thomas J. Moore in the *San Jose Mercury News*: "Unsafe Trucks Endanger Nation's Highways," Apr. 21, 1985; "Truck Safety Is Industry's Achille's Heel," Apr. 22, 1985; "U.S. Agency Puts Truckers on Easy Street," Apr. 23, 1985; and "U.S. Dodging Truck Safety Role," Apr. 24, 1985.

[19] Richard Ehlke, Legislative Attorney, American Law Division, Congressional Research Service, Library of Congress, telephone interview, Oct. 28, 1985.

[20] Dudley Clendinen, "New Computer Splits New Hampshire Officials," *New York Times*, date unknown.

Once the desired information has been identified and located, the next logical step would be to review how the committee intends to use the information (e.g., what kinds of statistical analyses are anticipated), and whether there is a significant advantage in providing the information to the committee directly in electronic form. Some information may not be suitable or usable for the purposes of the committee and/or for electronic transfer. In some cases, it may be preferable for the agency to do the analysis itself and submit a written report to the committee, or perhaps the committee will find that the agency has already carried out the desired analysis and need only provide a copy of an already existing report or other document.

Where desired information exists and the committee wishes to do its own analysis (or double-check the agency's work), then the relevant agency databases or files can be reviewed to ascertain the most cost-effective way to transfer the information—such as computer tape, computer disk or diskette, direct electronic linkage, or a paper printout. The information would then be transferred from the agency computer to congressional computers—probably either the mainframe computers in the Senate Computer Center or House Information Systems Office and/or microcomputers there or in committee offices.

The results of a series of pilot tests should provide a basis for developing standardized software and analytical protocols for committee access to computerized agency files and databases, and also help identify and resolve any procedural, legal, or jurisdictional issues that may arise.

Another complementary action that committees could take is requesting agencies within their jurisdiction to prepare and submit a listing or directory of all (or selected by issue) major files and databases maintained and update the directory on a regular basis. Alternatively, agencies could be asked to participate in any governmentwide indices or directories to agency databases that may be developed (see related discussion in ch. 7).

Computer-Based Modeling and Decision Support

Both the House Information Systems Office and Senate Computer Center offer assistance to Congress with respect to use of decision support software (e.g., spreadsheet and analytical packages) and the development and evaluation of computer models. However, use of these techniques appears to be quite limited, with the exception of economic and financial modeling.

The primary current congressional use of modeling tools is in the budgetary process "for evaluating funding alternatives, analyzing tax structures, and forecasting revenues and expenditures." Several computer-based large-scale econometric models are used, including Chase Econometrics, Wharton, Evans Economics, Merrill-Lynch Economics, Townsend Greenspan, and Data Resources, Inc. Several Federal agency models are also used for analysis of grant and expenditure levels for specific agency and government benefit programs.[21] CBO provides Congress with the results of various econometric models, an evaluation of these results, and a synthesis with assumptions and analyses that form the basis of CBO projections. This has had the effect of increasing the ability of Congress to act on budget matters more independently of the OMB estimates and projections. In the words of one congressional staff member:

> The major impact is that everyone is better informed. Less is done by stealth on the Hill today than in the past. The presence of CBO estimates and projections has done a great deal to keep OMB honest. We have taken some of the "crystal ball" out of the process. We are all professionals who attempt to understand how and why our projections differ.[22]

---

[21] Congressional Research Service, *Congressional Oversight*, op. cit., p. 70.

[22] Frantzich, "Congressional Applications," op. cit., p. 17.

The other congressional support agencies—OTA, GAO, and CRS—do make use of such techniques on an intermittent basis depending on the needs of specific studies or audits.

This report has documented (in ch. 6) the widespread Federal agency use of computer-based modeling and decision support. Agencies claim that much of this analytical work is being used in agency planning and policymaking. If so, then Congress may have unrealized opportunities to more effectively check and systematically evaluate the analytical basis for agency plans and policies.

Congress could plan for a small number of pilot tests in areas where agency plans and policies are clearly based on computer models and analyses, and where the authorizing or oversight committees have a desire to independently verify the models and analyses. Beyond this, Congress could develop a more extensive, ongoing capability for computer modeling and decision support. This could be a logical extension of expertise already resident in the Senate Computer Center, HIS, and the congressional support agencies.

The combination of access to agency electronic records and databases (discussed earlier) and use of computer-based analytical techniques can be very effective, as evidenced by the CBO experience with OMB budget and economic data and forecasts, and by the experience of several State legislatures, such as in New York and Washington:

- New York. The State legislature staff is one of the largest (4,000) and most sophisticated. Information technology has increased the volume of agency data directly accessible by legislative staff, and has reportedly limited the ability of agencies to manipulate the data before providing summaries to the legislature. Through the use of computers, staff are able to:
  —create their own databases with selected agency data, their own data, or both;
  —analyze the data through use of statistical software (e.g., Statistical Package for the Social Sciences); and
  —display the results of the analysis in bar graph, scatter plot, or spreadsheet format.[23]
- Washington. The State legislature has access to monthly expenditure, work load, and unit cost data for each major agency. Legislative staff analyze the data for any variance from budget and use spreadsheet software to present the results in graphic form to legislators. Information technology has helped staff perform such analyses more rapidly and thoroughly.[24]

Congress could also initiate a pilot test of the decision conference technique. This technique is intended to help the decisionmakers (e.g., individual Members of Congress or members of a congressional subcommittee or committee) and staff directly use computer-based analytical tools and models within their own decision framework. As discussed in chapter 6, OTA located one Federal agency that operates such a facility—the Office of Program Planning and Evaluation in the Department of Commerce. Commerce reports favorable results from the relatively few decision conferences conducted to date.

The basic idea would be to help Members and staff work through a decision problem in a reasonably structured way so that options and implications can be clearly identified and evaluated using the best available information. The information would be drawn from a wide variety of sources—prior studies, computerized databases, results of computer modeling, expert opinion, public opinion polls, key trends, and the like. Decision analytic tools (e.g., computer software, graphics) would be used on the spot, for example, to help structure and evaluate options.

Again, a logical first step would be for the participating committees to review their oversight responsibilities and current and prospective oversight issues, and make a preliminary identification of priority decision areas where further analytical support is thought to be helpful and needed. Each of the candidate decision areas could then be screened to select those where computer modeling and decision support techniques seem especially applicable, perhaps because agencies or others are already using these techniques or based on an independent assessment by congressional support staff.

---

[23] Miewald, "State Legislature," op. cit., pp. 26-31.
[24] Ibid., pp. 42-52.

For each decision area selected for a pilot test, a number of options could be considered. One option would be for the committees to request a report from the relevant agencies on the models, assumptions, data, and the like that were used in arriving at the agency position or decision. Alternatively, or in addition, where feasible the committees could request a copy of the software used by the agency so that the committee could run the model with its own set of assumptions and data and compare and contrast the results.

Another approach, not necessarily mutually exclusive, would be for committees to ask the agencies to use a previously agreed upon decision analytic framework in presenting decision information to Congress. The framework could specify, for each particular decision area, how options should be developed and evaluated, including the dimensions of evaluation that should be used and how qualitative factors are to be incorporated. This would not necessarily limit the agencies to only the specified decision analytic framework, but would provide a minimum set of requirements for congressional oversight purposes.

A further option, again not mutually exclusive with any of the above, would be for the committees to ask the Congressional Research Service to try preparing some issue briefs in a decision analytic framework, and the Congressional Budget Office to extend their budget and financial analyses to include other factors relevant to the decisions at hand. Thus, CRS could use various decision support models and techniques as adjuncts to the preparation of selected issue briefs in their standard format and in a "decision brief" format. CRS could also make the models available for use by committee staffs (perhaps in the form of diskettes to be used on personal computers), and possibly conduct seminars for Members and/or staffs on using computer-based decision support techniques.

As with committee access to agency files and databases discussed earlier, a complementary action that committees could take is requesting agencies within their jurisdiction to prepare and submit a listing or directory of major models and decision techniques used in selected priority decision areas. Again, agencies could be asked to participate in any governmentwide decision support directories or clearinghouses that may be established (see related discussion in ch. 6).

Finally, Congress may wish to consider establishing one or more "situation rooms" for congressional oversight use. These could be specially designed facilities where a broad range of computer and analytical tools, electronic databases, and computer graphics capabilities would be set up for real-time use by Members and staff. Several alternative configurations were discussed in chapter 6 under decision support and government foresight.

Video- and Computer-Conferencing

Congress already makes some use of new electronic communication techniques such as electronic mail. However, Congress makes very little use of video- and computer-conferencing—two other new techniques that offer significant oversight potential.

Videoconferencing is essentially two-way live television where participants at both locations can see and hear each other. Prior experiments with congressional videoconferencing have demonstrated both the technical feasibility and practical utility.[25] As early as 1977, a congressional subcommittee hearing was held with public testimony by two-way satellite videoconference.[26] In March 1985, OTA conducted a videoconference between Washington, DC, and Alaska.[27] Executive agencies report small but growing use of videoconferencing. In the private sector, the use of videoconferencing is rising, especially for business executives and key technical staff, as awareness and experience builds and costs drop.[28]

---

[25] Fred B. Wood, Vary T. Coates, Robert L. Chartrand, and Richard F. Ericson, *Videoconferencing Via Satellite: Opening Congress to the People*, Program of Policy Studies in Science and Technology, The George Washington University, Washington, DC, April 1979. Also see Fred B. Wood, "Congressional Perceptions of Emerging Telecommunications," *Technological Forecasting and Social Change*, vol. 8, 1975, pp. 189-212; and Fred B. Wood, "Congressional-Constituent Telecommunication: The Potential and Limitations of Emergent Channels," *IEEE Transactions on Communications*, vol. 23, No. 10, October 1975, pp. 1134-1142.

Given the heavy time pressures on Members of Congress and their staffs, and the substantial costs associated with travel (whether by witnesses coming to Washington, DC, or Members going to field locations), videoconferences warrant consideration as an option. Based on current commercial charges, simple videoconferences between two locations with permanent studios can be arranged for $500 to $1,000 per hour, depending on the geographic distance and time of day. Costs are expected to drop in the future, as the range of videoconferencing options expands.

Implementation alternatives for pilot tests of videoconferencing are straightforward, since there is already a history of successful demonstrations. Pilot tests could be run using a variety of commercial services, with congressional participants using existing facilities either in downtown Washington, DC, studio locations or in the House and Senate recording studios. The technical and cost aspects of possible videoconferencing pilot tests could be worked out by congressional support office staff, in consultation with commercial vendors. The subject matter of the pilot tests presumably would be largely up to the participating committees or subcommittees, who could be invited to identify a list of oversight topics where face-to-face input from and discussion with out-of-town persons would be helpful. Hopefully, the pilot tests actually conducted would be those with a favorable benefit/cost ratio, that is, where the actual costs of the videoconference would be significantly less than the costs of travel and related expenses for witnesses.

With respect to computer conferencing, the commercially available options are even more diverse, geographic location is not a constraint as long as the participants have a computer terminal with a communications link, and cost is minimal (e.g., $10 to $30 per connect hour).[29] Computer-conferencing could have across-the-board applications in Congress, but particularly with respect to legislative and oversight functions. Computer-conferencing makes it possible for Members and staff to establish ongoing "electronic discussions or meetings" with interested persons around the country. Computer-conferencing is becoming more feasible as the number of congressional offices and interested citizens with computer terminals increases.

Another option to encourage computer-conferencing would be to ensure that House and Senate computers (and perhaps executive agency computers) are technically compatible. This could be viewed as an extension of existing electronic mail capabilities. Apparently, at present, most House office computers can communicate electronically among themselves, but not with Senate or executive branch office computers. Nor can many Senate office computers communicate. Removal of these technical barriers would presumably encourage congressional computer-conferencing.

---

[26] Ibid., pp. 9-12.

[27] OTA held a 2-hour videoconference on Mar. 29, 1985, between Washington, DC, and Anchorage and Juneau, Alaska. Videoconference studio facilities and the satellite link were provided as a public service by ARCO Corp. Participants included congressional staff in Washington, DC, and State and local government officials at the Alaska locations.

[28] See for example, Gordon Heffron, "Teleconferencing Comes of Age," *IEEE Spectrum*, October 1984, pp. 61-66; "Videoconferencing: No Longer Just a Sideshow," *Business Week*, Nov. 12, 1984, pp. 116-120; Susanna Opper and A. David Boomstein, "Video Teleconferencing—Corporations Conquer Distance," *Computer Decisions*, Nov. 15, 1984, pp. 62-68; Earle Adams, "Videoconferencing via Voice and Data Circuits," *Telecommunications*, February 1985, pp. 119a-120a; "Videoconference 'Co-op' Looks Like Key to Success," *Data Communications*, April 1985, pp. 60-64; M. Fentress Hall, "Case History: Video Teleconferencing at NASA," *Telecommunications*, June 1985, pp. 80-80c; and John Tyson, "Cutting Costs, Boosting Productivity: It's Happening Slower Than Predicted, But Videoconferencing Use Is Increasing in Business Today," *Satellite Communications*, November 1985, pp. 39-42.

[29] See for example, C. Jackson Grayson, Jr., "Networking by Computer," *The Futurist*, June 1984, pp. 14-17, and, in general, the special section on "Networking," pp. 9-23; Dennis Livingston, "Computer Conferencing," *Datamation*, July 15, 1984, pp. 111ff; Alex Czajkowski and Sara Kiesler, "Computer-Mediated Communication," *National Forum*, summer 1984, pp. 31-34; Richard T. Rodgers, "ABA net: A User's Report," *Legal Economics*, May/June 1985, pp. 48-49; Andres Llana Jr., "Get Face-to-Face With Efficient Business Communications," *Communication Age*, August 1985, pp. 32-33; and "PARTICIPATE: The Advanced Computer Teleconferencing System," Participation Systems, Inc., no date.

Some illustrative topics for computer-conferencing include:

- obtaining comments on draft legislation;
- exchanging ideas on possible new legislative and oversight initiatives;
- identifying possible subjects for congressional committee oversight;
- keeping track of key trends and issues relevant to committee oversight jurisdiction;
- keeping track of key trends and issues in specific geographical and/or subject areas;
- obtaining comments on draft committee oversight or legislative reports;
- exchanging ideas on implementation of public laws;
- keeping track of agency performance;
- monitoring research results relevant to committee jurisdiction; and
- monitoring key meetings, conferences, and activities that may be of interest.

Again, a series of congressional pilot tests or demonstrations appears to be a reasonable way to proceed, in order to flesh out the benefits, costs, and possible pitfalls. Any such tests could benefit from the substantial body of prior research on computer conferencing.[30]

Electronic Tracking of Agency and Executive Actions

Congress frequently requests or directs specific agency actions through public law, and through authorizations, appropriations, and oversight hearings and reports. To a significant degree, monitoring of agency compliance with congressional requests or directives is on an exception basis, given the large volume of items and competing demands for congressional attention. The potential for computer-assisted monitoring seems significant, both for tracking: 1) agency compliance with specific actions mandated by Congress; and 2) significant agency action bearing on the intent and/or effects of legislation. The House Information Systems Office has already implemented one such system—for tracking receipt of legislatively mandated reports to Congress.[31]

A variety of pilot tracking applications could be developed. Each participating committee or subcommittee could identify and develop a list of key agency action items mandated by law or other congressional action within the committee's jurisdiction. These items could then be put into a computer program that would automatically flag items when due and note their status as being "on schedule," "overdue," "rescheduled," "unknown," and so forth, based on either direct electronic agency input or committee staff input derived from agency submissions. The results of this tracking process could provide one basis for committee oversight of trouble spots and overall agency performance, investigation of any areas of serious noncompliance, reevaluation of action items whose utility may have passed or been misjudged from the beginning, and, indeed, commendation for exemplary agency performance in carrying out congressional intent.

---

[30] See, for example, the special section on "Person-to-Person Networks," *Bulletin of the American Society for Information Science*, June 1978, pp. 9-23, including articles by Murray Turoff, "The EIES Experience: Electronic Information Exchange System"; Starr Roxanne Hiltz, "Controlled Experiments With Computerized Conferencing"; Peter Johnson-Lenz, et al., "How Groups Can Make Decisions and Solve Problems Through Computerized Conferencing"; and Jacques Vallee, et al., "Computer Conferencing: The Management Issues." Robert Johansen, Jacques Vallee, and Kathleen Spangler, *Electronic Meetings* (Reading, MA: Addison-Wesley, 1979); Elaine H. Kerr and Starr Roxanne Hiltz, *Computer-Mediated Communication Systems: Status and Evaluation* (New York: Academic Press, 1982); Starr Roxanne Hiltz, *Online Communities: A Case Study of the Office of the Future* (Norwood, NJ: Ablex Publishing, 1984); Starr Roxanne Hiltz and Murray Turoff, "Structuring Computer-Mediated Communication Systems to Avoid Information Overload," January 1984; Robert Johansen and Christine Bullen, "What To Expect From Teleconferencing," *Harvard Business Review*, March-April 1984, pp. 4-10; Starr Roxanne Hiltz, "Computer Networking Among Executives: A Case Study of the White House Conference on Productivity," June 1984; Robert M. Fano, "Computer-Mediated Communication," *IEEE Technology & Society Magazine*, March 1985, pp. 3-6; and Edward G. Canning, "More Uses for Computer Conferencing," *EDP Analyzer*, August 1985.

[31] Boyd Alexander, House Information Systems Office, letter to Fred Wood of OTA, Nov. 15, 1985.

Finally, a computerized tracking system could be devised to help participating committees and subcommittees monitor key trends and developments, including agency activities, relevant to their jurisdiction. This could be a form of early warning of possible emerging problems and issues that warrant congressional attention, but otherwise might escape the notice of the traditional oversight process.

Appendixes

Appendix A

Other Issues

The following issues are not within the primary focus of this report. Some are addressed in related OTA reports or studies. All warrant congressional attention.

Electronic Communications Security and Privacy

The importance of technical, administrative, and legal measures to maintain computer security was discussed earlier. Equally important is the security of the communication lines and networks used to transmit information between and among computers, terminals, and the like. Privacy (as well as, potentially, national security) can be compromised if either computer or communications security is breached.

In a related, prior study entitled *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* (October 1985), OTA found that many new electronic communication technologies are ambiguously covered or not covered at all by existing privacy law. For example, existing law offers little or no protection against interception of electronic mail, data communication between computers, and digital transmission of video and graphic images. OTA also found that about 25 percent of Federal agency components use or plan to use electronic surveillance technologies, many of which also are not clearly covered by existing law. One of several options available to Congress is to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the approach taken in H.R. 3378 and S. 1667, the Electronic Communications Privacy Act of 1985. See OTA's report for further discussion. Although there is no immediate technical answer to protection against electronic surveillance, technical options are being addressed in a separate OTA study, *New Communications Technology: Implications for Privacy and Security* (forthcoming in late 1986).

Electronic Record Systems Privacy

The privacy of information stored in Federal Government record systems is protected in part by the same measures used to provide computer and communications security. However, these measures are directed against unauthorized access or misuse and abuse by authorized users. With respect to Federal record systems, new kinds of authorized uses (e.g., computer matching of records in two or more Privacy Act record systems, use of the social security number as a de facto national electronic identifier) far exceed those envisioned when Congress enacted the Privacy Act of 1974. While information technology offers many new opportunities to improve the efficiency of government recordkeeping and help prevent and detect fraud, waste, and abuse, the technology also presents new possibilities for inappropriate use or abuse of personal information. Relevant trends, issues, and policy options are discussed in OTA's forthcoming 1986 report entitled *Federal Government Information Technology: Electronic Record Systems and Individual Privacy.*

Office Automation Impacts and Issues

This study considered office automation technologies—such as word processing, electronic mail, and optical disks—to the extent such technologies are subsumed within information technology management or IRM. However, office automation also is likely to have very specific impacts in areas such as the number, type, and content of office jobs; organizational structure; quality of worklife; and employee health and safety. These have been comprehensively studied in a December 1985 OTA report entitled *Automation of America's Offices.*

Institutional Change in Federal Information Technology Management and Policymaking

Over the last several years, a growing number of Members of Congress, industry leaders, and researchers have concluded that institutional change is needed in addition to legislative action and policy guidance on specific issues. Institutional change can itself focus on specific areas, such as strengthening the roles of the National Bureau of Standards and the National Security Agency in information systems security (see ch. 4), or establishing a new Data Protection Board or Privacy Protection Commission[1] to oversee Privacy Act implementation (see extensive discussion in OTA,

---

[1] See H.R. 1721, the Data Protection Act of 1985.

Electronic Record Systems and Individual Privacy, forthcoming 1986).

Institutional change can also focus on a broader range of issues. Options not considered in this study but deserving attention include:

- upgrading the Information Policy Branch of the Office of Management and Budget's Office of Information and Regulatory Affairs;
- reestablishing an Office of Telecommunications Policy (or the equivalent, e.g., an Office of Federal Information Policy) in the Executive Office of the President as a separate office or perhaps as part of the Office of Science and Technology Policy;[2]
- establishing an Institute for Information Technology Research and Innovation (or the equivalent) in the executive branch (see related discussion in ch. 3);[3]
- combining roles and resources from several agencies (e.g., the Office of Management and Budget, the General Services Administration, the National Bureau of Standards) into a new Federal information management agency; and
- creating a new study commission on national information technology and policy issues.[4]

International Information Management and Policy

While this study focuses on national—and even more narrowly, Federal—information technology, management, and policy trends and issues, information technology knows no boundaries. The international flow of information over computerized data, voice, and video networks is essential to the national economy, international trade and diplomacy, and national security. Canada, Japan, and many European nations have well-developed national information policies, and many other nations are establishing such policies. Therefore, U.S. policymakers need to consider the international implications of domestic management and policy initiatives on information technology.[5]

---

[2] See, for example, H.R. 642, the Telecommunications Policy Coordination Act of 1985.

[3] See, for example, H.R. 744, the Information Science and Technology Act of 1985.

[4] See S. 786, the Information Age Commission Act of 1985. Also see the proposal of the Association of Data Processing Service Organizations for a "Temporary National Information Committee," and the "Panel on National Information Issues" formed by the American Federation of Information Processing Societies.

[5] A separate OTA study on *International Competition in the Services Industries* (forthcoming 1986) is examining technical, trade, and policy issues involving data processing and information services, computer software, and telecommunications.

Appendix B

OTA Federal Agency Data Request

After reviewing all available sources of information on Federal use of information technology, OTA determined that important information was not available in certain areas critical to the OTA assessment. To meet the need for additional information, OTA drafted a request for current agency data covering the areas in which information was lacking or incomplete. The draft request was reviewed by congressional staff of interested committees, and then pretested in four agencies—the Energy Information Administration (Department of Energy), the Food and Nutrition Service (Department of Agriculture), the Office of the Assistant Secretary for Postsecondary Education (Department of Education), and the Veterans Administration. Based on the results of the pretest, the data request was revised. (See attachment 1 for portions of the final, revised data request relevant to this report).

In April 1985, the data request was sent to the 13 cabinet-level agencies and 20 selected subcabinet agencies (see attachment 2) with a turnaround time of 5 weeks. Sufficient copies were provided for each of the subcomponents of the cabinet agencies. Agencies were informed that no new data collection was to be conducted. An OTA staff member was identified who could be contacted to provided clarification where necessary.

All agencies that were sent the request provided a response, although the responses varied in completeness and quality. A total of 142 agency components provided information. While many of the agencies provided responses well within the time allotted, the completion time for the entire request (142 agency components) was approximately 2 months. The data provided were compiled by OTA staff and appear as appropriate throughout the report.

A draft copy of the OTA report was provided to each of the participating agencies for review and comment.

Attachment 1

OTA FEDERAL AGENCY DATA REQUEST

INFORMATION TECHNOLOGY MANAGEMENT

A. Please provide the following technology data, to the extent available, for fiscal years 1975 (actual), 1980 through 1984 (actual by year), and 1985 (planned).

	1975	1980	1981	1982	1983	1984	1985
Technology (number of units in use by year)							
1. mainframe computers-- a)systems							
b)central processing units							
2. terminals for mainframe computers							
3. microcomputers (use (GSA definitión*)							
4. telephones							

B. Please provide a copy of your agency's most recent 5-year plan and any other current planning document for information technology (e.g., automated data processing, microcomputers, and telecommunications).

C. For your agency's mainframe computers (i.e., major system acquisitions), please provide data, to the extent available, on the average age (in years/months) of operating mainframes and average procurement time (in years/months) of mainframes purchased in 1975, 1980, and 1984 (by year).

	1975	1980	1984
Average age			
Average procurement time			

D. Please list the major factors that are affecting (e.g., increasing or decreasing) the average procurement time for mainframe computers.

---

*The GSA definition of microcomputer is: Any microprocessor-based work station capable of independent use--including stand-alone and networked "personal computers," "professional computers," "intelligent terminals," word processors, and other similar devices--costing less than $10,000 per unit, but excluding peripherals and separately purchased software.

E. Please indicate which, if any, of the following technologies your agency has used, is using, or is planning to use:

	Past Use		Current Use		Planned Use	
	Yes	No	Yes	No	Yes	No
Audio-conferencing	___	___	___	___	___	___
Teleconferencing (1-way video, 2-way audio)	___	___	___	___	___	___
Videoconferencing (2-way video)	___	___	___	___	___	___
Computer-conferencing	___	___	___	___	___	___
Teletext	___	___	___	___	___	___
Videotext	___	___	___	___	___	___
Cable television	___	___	___	___	___	___
Interactive cable TV	___	___	___	___	___	___
Expert systems/artificial intelligence	___	___	___	___	___	___
Electronic mail	___	___	___	___	___	___
Voice mail	___	___	___	___	___	___
Optical disks	___	___	___	___	___	___

F. For any technologies checked "yes" in question E above, please describe, to the extent feasible, the specific technology, application(s), users (or participants), location(s), date(s), costs, and results (or evaluation). Please provide a copy of any written reports on these uses.

G. Has your agency conducted one or more information security risk analyses of computer/telecommunications systems since 1980? Yes ___ No ___ If yes, please provide data, if available, on the number of risk analyses conducted per year for the fiscal years 1980 and 1984. Please provide data, if available, on the average and high/low cost per risk analysis by year. Please provide a copy of your agency's three most recent computer (and telecommunications) security risk analyses.

H. Please indicate which, if any, of the following or other security techniques are used by your agency for protection of sensitive unclassified information.*

	Yes	No	If Yes, for what % of systems that process sensitive unclassified information?
Applications screening (i.e., management certification)	___	___	____%
Personnel screening	___	___	____
Audit software (i.e., audit trails)	___	___	____
Restrictions on dial-up access	___	___	____
Password controls on access	___	___	____
Encryption	___	___	____
Back-up hardware	___	___	____
Back-up of key data files	___	___	____
Physical security for hardware	___	___	____
Other ____________	___	___	____

I. Does your agency have an explicit information security policy for microcomputer users? Yes ___ No ___. If yes, please attach a copy of your agency's security policy for microcomputers.

J. Please indicate which, if any, of the following have provided your agency with assistance in developing security plans and policies during fiscal years 1983, 1984, or 1985, and the date and nature of this assistance.

	Yes	No	If Yes, provide date and describe nature of assistance
OMB	___	___	____________
GSA	___	___	____________
NBS	___	___	____________
NSA	___	___	____________
DOD Computer Security Center	___	___	____________
Other Federal (specify)	___	___	____________
Private contractor (specify)	___	___	____________
Other non-Federal (specify)	___	___	____________

---

*Sensitive unclassified information: information collected, maintained, and/or disseminated by an agency that is not classified but whose unauthorized release or use could compromise or damage privacy or proprietary rights, critical agency decisionmaking, and/or the enforcement or implementation of public law or regulation under which the agency operates.

K. Does your agency have a contingency plan for handling disruption of your major mainframe computer systems by external factors, (e.g., electric power failure, data network interruption, natural disaster, sabotage)? Yes ___ No ___. If yes, please provide a copy.

L. Please provide data, to the extent available, on your agency's funding and staffing (in full-time equivalents) for computer and communications security for fiscal years 1975 and 1980 through 1985.

	1975	1980	1981	1982	1983	1984	1985
Funding (current dollars)	___	___	___	___	___	___	___
Staff (full-time equivalents)	___	___	___	___	___	___	___

M. Does your agency have an established procedure for tracking and analyzing computer-related crime in your agency? Yes ___ No ___. If yes, please describe in detail. In either case, please provide your agency's best estimate, to the extent feasible, of the number and type of computer-related crimes for 1984; indicate whether the perpetrator was an agency employee, a Federal employee from another agency, a Federal contractor employee, or a person not associated with the Federal Government; indicate whether criminal, civil, and/or administrative proceedings were initiated; and provide the results thereof.

N. Does your agency have an established policy on employee access to agency computers (e.g., what employees are authorized to access which computers)? Yes ___ No ___. If yes, please describe in detail, including a description of the criteria on which determinations of employee authorizations are based. Does the policy extend to employee access to microcomputers? Yes ___ No ___. If yes, please provide details.

PUBLIC INFORMATION

A. Please provide budget, staffing, and activity data, to the extent available, for fiscal years 1980 and 1984 (actual by year), 1985 (projected), and 1986 (anticipated) for your agency's public information activities, defined to include:

1. Printing and publishing (e.g., number of titles, total copies, total pages, fee or free). Break out in-house, contractors, etc.
2. Public affairs (e.g., number of conferences, seminars, and/or workshops on information dissemination and public access and awareness of agency information)
3. Libraries and information centers (e.g., number of libraries, number of information centers or clearinghouses). Break out in-house, contractors, etc.
4. Statistical activities (e.g., number of surveys, average sample size). Break out in-house, contractors, etc.

B. Has your agency compiled any data or conducted or sponsored any studies on the impact of any changes in your public information activities on user groups, agency clients, and/or the general public? Yes ___ No ___. If yes, please provide copies of such materials. If no, please describe any plans to compile such data or conduct or sponsor such studies.

C. Does your agency have a directory or catalog of your public information activities and products? Yes ___ No ___. If yes, please provide copies. If no, please describe any plans to compile such a directory or catalog.

D. Does your agency make available or disseminate any public information in electronic format (e.g., computer tape or disk, direct electronic)? Yes ___ No ___. If yes, please provide further details below. If no, please describe any plans to disseminate electronically.

E. For each specific public information product (e.g., report, data base, statistical series) available in electronic format, please provide the following information, to the extent available:

1. Name of public information product and startup date
2. Statutory or regulatory authority or requirement, if applicable
3. Brief description of product (e.g., size and contents of data base)
4. Type of electronic format (e.g., computer tape or disk, direct electronic, dial-up access)
5. Information available: directly from Government agency, from Government contractor, from commercial vendor, or combination (please specify)
6. Number of users per year for fiscal year 1984

7. Type of users if known (e.g., general public, university researchers, libraries, State/local governments, business corporations, public interest groups, trade associations) with percentage of 1984 total use by type of user
8. Fee schedule (e.g., free, subscription, one-time use fee) and typical charges
9. Currently available in paper form? Yes ___ No ___. If yes, what is the cost? If no, was the product previously available in paper form, and if so, what did it cost and when was it terminated?
10. If your agency is providing public information in electronic format instead of paper format, please list and discuss the reasons why (e.g., comparative cost, user preference, competing products)

F. Has your agency conducted or sponsored any studies on the impact of provision of public information in electronic form? Yes ___ No ___. If yes, please provide copies of such studies. If no, please describe any plans to conduct or sponsor such studies.

G. Does your agency have any specific policies or procedures on provision of public information (e.g., with respect to fee schedules, cost recovery, contracting out, mode of access, private sector provision)? Yes ___ No ___. If yes, please provide a copy.

H. Does your agency conduct activities designed to increase public awareness of, access to, or use of your public information? Yes ___ No ___. If yes, please list and describe these activities. If no, please describe any plans to conduct such activities.

I. Does your agency make any use of remote printing or printing-on-demand technology (e.g., printing out copies of reports only as requested and/or at remote, decentralized locations)? Yes ___ No ___. If yes, please provide detailed information on the specific use, extent of use, location(s), and cost. If no, please describe any plans to use such technology.

COMPUTER-BASED DECISION SUPPORT

A. Does your agency use computer-based modeling (including simulation) to support agency activities and programs (including decisionmaking on Federal Government policies and programs within your agency's jurisdiction)? Yes ___ No ___. If yes, please provide the detailed information below.

B. Does your agency have a directory of modeling applications within your agency? Yes ___ No ___. If yes, what is the format of the directory (e.g., paper, microfiche, on-line electronic, computer tape)? If the directory is in paper or microfiche format, please provide a copy (paper preferred).

C. Does your agency have a clearinghouse or other central reference point (e.g., a person or organizational unit that maintains current information) about modeling applications? Yes ___ No ___. If yes, please identify the clearinghouse (or person's) name, location, and telephone number.

D. Does your agency have procedures or policies on the availability of modeling details (e.g., structure, assumptions, input data) to the public? Yes ___ No ___. To Congress? Yes ___ No ___. If yes, please provide a copy of such procedures or policies.

E. Has your agency conducted or sponsored any studies on the impact or use of modeling to support agency decisionmaking? Yes ___ No ___. If yes, please provide copies of such studies.

F. Please estimate the total number of modeling applications used in 1984, and list the 10 areas of application (e.g., estimate air pollution levels, project future level of Medicare/Medicaid beneficiaries, simulate climatic change) with the heaviest use.

1984 total applications ______
10 heaviest areas of application:

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________
5. ______________________________
6. ______________________________
7. ______________________________
8. ______________________________
9. ______________________________
10. ______________________________

G. Please indicate which, if any, of the following computer-assisted decision analytic techniques your agency is using or is planning to use:

	Current Use		Planned Use	
	Yes	No	Yes	No
Spreadsheet software (e.g., Lotus 1-2-3, VisiCalc)	___	___	___	___
Forecasting techniques (e.g., Delphi)	___	___	___	___
Quantitative decision analytic techniques (e.g., linear programming, queuing analysis, systems analysis, critical path analysis)	___	___	___	___
Quantitative decision analytic techniques with judgmental input (e.g., decision trees, subjective probability, multi-attribute utility)	___	___	___	___
Decision conference techniques (e.g., interactive use of computer assisted analytical techniques by decisionmakers in group situation)	___	___	___	___
Electronic voting techniques (e.g., consensor)	___	___	___	___
Computer-conferencing for decision analysis	___	___	___	___
Other ______________________	___	___	___	___

H. For any techniques checked "yes" in question G above, please describe, to the extent feasible, the specific technique, application(s), user(s), costs, and results (or evaluation). Please provide a copy of any written reports on these uses.

I. Does your agency have the following:

	Yes	No
Directory of decision analytic techniques	___	___
Clearinghouse of decision analytic techniques	___	___
Decision analytic support center	___	___

If yes to any of the above, please provide copies of relevant descriptive documents and the names, locations, and telephone numbers of knowledgeable persons. If no to all of the above, please describe any plans to initiate such activities.

J. Has your agency conducted or sponsored any studies on the impact of using decision analytic techniques to support agency decisionmaking?
Yes ___ No ___. If yes, please provide copies of such studies.

Attachment 2

Federal Departments and Agencies
Responding to OTA Data Request

Cabinet Department	Number of Agency Components Responding
Agriculture	25
Commerce	17
Defense	14
Education	2 (agency-wide)
Energy	3 (EIA, FERC, and rest of agency)
Health and Human Services	9
Housing and Urban Development	1 (agency-wide)
Interior	9
Justice	13
Labor	8
State	1 (agency-wide)
Transportation	11
Treasury	9
Subtotal	122
Independent Agencies	
Commission on Civil Rights	1
Consumer Product Safety Commission	1
Environmental Protection Agency	1
Equal Employment Opportunity Commission	1
Federal Communications Commission	1
Federal Elections Commission	1
Federal Emergency Management Agency	1
Federal Reserve System	1
Federal Trade Commission	1
General Services Administration	1
National Aeronautics and Space Administration	1
National Archives and Records Administration	1
Nuclear Regulatory Commission	1
Securities and Exchange Commission	1
Selective Service System	1
Small Business Administration	1
Arms Control and Disarmament Agency	1
U.S. Information Agency	1
Agency for International Development	1
Veterans Administration	1
Subtotal	20
TOTAL	142

Appendix C

List of Contractor Reports

Copies of the following contractor reports completed in support of this assessment are available from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161, (703) 487-4650.

1. Rex V. Brown, *Personalized Decision Analysis As An Expert Elicitation Tool: An Instructive Experience in Information Security Policy* (Feb. 25, 1985); *A Brief Review of Executive Agency Uses of Personalized Decision Analysis and Support* (Mar. 14, 1985); *Selected Applications of Computer-Aided Decision Analysis* (May 10, 1985); and *Decision Analysis As a Tool of Congress* (May 10, 1985), all prepared for OTA by Decision Science Consortium, Inc.
2. Stephen Frantzich, *Congressional Applications of Information Technology*, prepared for OTA by Congressional Data Associates, February 1985.
3. Henry H. Hitchcock, Lisa Heinz, and Joseph F. Coates, *Scenarios of Five Federal Agencies (1991-95) As Shaped By Information Technology*, prepared for OTA by J.F. Coates, Inc., June 21, 1985.
4. Kenneth L. Kraemer, John Leslie King, and David G. Schetter, *Innovative Use of Information Technology in Facilitating Public Access to Agency Decisionmaking: An Assessment of the Experience in State and Local Governments*, prepared for OTA by the Irvine Research Corp., March 1985.
5. John C. Kresslein, *A Comparative Review of Information Technology Management Practices in Selected State Governments*, prepared for OTA by the Institute of Information Management, Technology and Policy, College of Business Administration, University of South Carolina, December 1984.
6. Karen B. Levitan, Patricia D. Barth, and Diane Griffin Shook, *Agency Profiles of Civil Liberties Practices*, prepared for OTA by the KBL Group, Inc., Dec. 28, 1984.
7. Charles R. McClure and Peter Hernon, *Federal Government Provision of Public Information: Issues Related to Public Access, Technology, and Laws/Regulations*, prepared for OTA by Information Management Consultant Services, Inc., Dec. 28, 1984.
8. Robert Miewald, Keith Mueller, and Robert Sittig of the University of Nebraska-Lincoln, *State Legislative Use of Information Technology in Oversight*, prepared for OTA, January 1985.
9. Sanford Sherizen, *Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options*, prepared for OTA by Data Security Systems, Inc., February 1985.

Appendix D

Other Reviewers and Contributors

Ralph W. Adams
National Security Agency

Margaret Alter
Internal Revenue Service

Gerald Barney
Global Studies Center

Roger G. Barry
University of Colorado

Danny J. Boggs
U.S. Department of Energy

Alden Bryant
Earth Regeneration Society

Daniel Burk, Esq.
Cadwalader, Wickersham, & Taft

Center for Climatic Research
University of Wisconsin:
  Reid A. Bryson
  John Kutzbach

Bob Chen
University of North Carolina and National Academy of Sciences

Congressional Research Service:
  John Justus
  Dan Melnick
  Sandra Milevski
  Fred Pauls
  Harold Relyea

Eileen D. Cooke
American Library Association

Robert H. Courtney, Jr.
RCI

Mary Culnan
The American University

Robert E. Dickinson
National Center for Atmospheric Research

Federal Bureau of Investigation:
  William A. Bayse
  Stephen W.C. Holbrook
  Thomas Walczykowski

Donald E. Fossedal
U.S. Government Printing Office

John J. Franke, Jr.
U.S. Department of Agriculture

General Services Administration:
  Francis A. McDonough
  David Mullins
  Donald Page
  Neil Stillman

Lindsay Grant
U.S. Department of State (ret'd)

M. Blake Greenlee
Citicorp Information Systems

Edward J. Hanley
Environmental Protection Agency

Ronald H. Hinckley
National Strategy Information Center

Diane Holt
Wesleyan University

Sherwood B. Idso
U.S. Department of Agriculture

J.E. Ingram
IBM Corp.

George Kukla
Columbia University

Robert Lamson
National Science Foundation

Alan S. Miller
World Resources Institute

National Computer Security Center:
  Anne J. Cuomo
  Jeff Chandler

Fred A. Newton III
Federal Emergency Management Agency

Michael Nugent
Electronic Data Systems

Hugh O'Neill
U.S. Department of Health and Human Services (formerly)

David Plocher
OMB Watch

Chester F. Ropelewski
National Oceanic and Atmospheric Administration

Ralph Schofer
National Bureau of Standards

Ronald M. Scroggins
Nuclear Regulatory Commission

Jack J. Sharkey
Veterans Administration

Ollie Smoot
Computer and Business Equipment Manufacturers Association

George Sotos
U.S. Department of Education

Patricia G. Strauch
Mead Data General

U. S. Department of Commerce:
  Jimmie D. Brown
  Chris Kyriazi

U. S. Department of State:
  William L. Ball, III
  Kenneth R. Erney

U.S. Department of Transportation:
  Bradley H. Hoke
  John E. Turner

U.S. Department of the Interior:
  Oscar W. Mueller, Jr.
  Leon W. Transeau

U. S. General Accounting Office:
  Morey Chick
  Harold J. Podell

U.S. Geological Survey
U. S. Department of the Interior:
  Richard S. Williams, Jr.
  Ethan T. Smith

Kenneth E.F. Watt
University of California at Davis

Frederic G. Withington
Arthur D. Little, Inc.

Ken Wong
BIS Applied Systems, Ltd.

U.S. GOVERNMENT PRINTING OFFICE : 1986 O - 57-461 : QL 3

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a non-voting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications, food and renewable resources; health; communication and information technologies; oceans and environment; and science, education, and transportation.